Splunk Logging as a Service (LaaS) Use Cases

Version Number: 1.27 – August 20, 2018

Version Control Page:

Date	Version	Name of Person Making Change	Description of Changes
August 16, 2016	0.1	David Lachmansingh (Richter)	Initial Draft
December 14, 2016	0.2	David Lachmansingh (Richter)	Updated to reflect approvals of use cases
January 3, 2017	0.3	Mark Walsh (Richter)	Updated to incorporate relevant section of 'CSOC Log Review – Exception Report Handling' document for consolidation purposes
January 6, 2017	0.4	Mark Walsh (Richter)	Updated based on feedback
June 23, 2017	1.0	David Lachmansingh (Richter)	Updated approvals and finalized document
October 3, 2017	1.1	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated approvals and provided cosmetic changes to document for presentation
October 4, 2017	1.2	David Lachmansingh (Richter, PM) Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated document to include 'Scope' section as per Christine Dewhurst
October 4, 2017	1.2	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM25.2 to reflect Critical Device Threshold increase from 5 to 12 hours as per CRUCM315
November 6, 2017	1.3	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM31.4 specific to Functional ID identification and actions to be taken by Log Reviewers
November 20, 2017	1.4	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM13.1, UCM13.2, and UCM24.1 to reflect ownership change to TBCG for Exception Reports (Alerts). Also updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM
December 7, 2017	1.5	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM31.2 to reflect Decommissioning of UCM for Network Devices. Use Case Status provides rationale
December 8, 2017	1.6	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM12.1, UCM12.2, UCM13.14c, UCM31.5, UCM31.5a, and UCM31.5b to reflect change of iSeries exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM. Reference CRUCM479 (12.1 & 12.2), CRUCM480 (31.5), CRUCM481 (31.5a & 31.5b), and CRUCM482 (13.14c)
December 12, 2017	1.7	Mark Walsh (Richter, BA)	Updated UCM24.1 for iSeries to reflect specific actions to be taken when events are captured pertaining to the use of the QSECOFR account
December 14, 2017	1.8	Mark Walsh (Richter, BA)	Updated UCM12.1 for Windows/*nix to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM. Reference CRUCM492. Updated UCM25 to reflect enhancements, including Remedy ticket generation throttling, anti-duplication, exception lookups, active/passive clustering, automated Remedy ticket closure, and intelligent delays
December 15, 2017	1.9	Anthony DeMedeiros (Manager, LaaS-TBCG)	Added "Review Date Status" section to individual Use Cases for annual reviews

December 20, 2017	1.10	Mark Walsh (Richter, BA)	Updated UCM12.1 for Oracle to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM498)
January 4, 2018	1.11	Mark Walsh (Richter, BA)	Updated UCM12.1 for Networks to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM504) Updated UCM12.1 for Applications to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM505) Updated UCM12.2 for Applications to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM506) Updated UCM24.1 for *nix to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM507) Updated UCM13.14a for iSeries to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM508)
January 8, 2018	1.12	Mark Walsh (Richter, BA)	Updated UCM 12.1, 12.2, 13.14a and 34 for PostgreSQL to reflect change of exception reports to alerts. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM511) Updated UCM 12.1 for SQL to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM514) Updated UCM 12.1 for Sybase to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM515)

January 17, 2018	1.13	Mark Walsh (Richter, BA)	Updated UCM 12.2 for MSSQL to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM524) Updated UCM 12.2 for Oracle to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM525) Updated UCM 34 for iSeries to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM529) Updated UCM 12.2 for Sybase to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM532) Updated UCM 24.1 for Windows to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM533)
January 18, 2018	1.14	Anthony DeMedeiros (Manager, LaaS-TBCG)	As per IMRR RRS requirements for Logging & Reporting retention, changed retention period from 14 months to 24 months as per RRS – 1ADM25
January 25, 2018	1.15	Mark Walsh (BA, Richter)	Updated UCMs 12.1, 12.2, 13.3, 13.4, 13.14a, 31.3, and 34 to include Tandem and include actions to be taken by Log Reviewers
February 7, 2018	1.16	Anthony DeMedeiros (Manager, LaaS-TBCG)	Added contextual direction for UCM 24.2 specific to the inclusion of “Failed” attempts to access security logs as part of the Log Reviewers review/analysis of users activities (Anomaly #2)
February 12, 2018	1.17	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM 13.6 to provide further direction for Log Reviewers on the use of UCM 13.6a report (Internal to External – High Risk) as a compliment to the UCM 13.6 report
February 13, 2018	1.18	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM 31.2c (*nix) to provide further direction for Log Reviewers on the use of UCM 31.2c report (“su” or “sudo” commands where the source user is not “root” – High Risk) as a compliment to the UCM 31.2r (*nix) report (“su” or “sudo” commands where the source and destination users are “root”)

February 14, 2018	1.19	Mark Walsh (BA, Richter)	Updated UCM 24.1 for Networks to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM601) Updated UCM 31.2 for Oracle to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM602) Updated UCM 13.15 for Windows Domain to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM603) Updated UCM 13.1 for Applications to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM604) Updated UCM 13.14a for Sybase to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM606) Updated UCM 34.1 for Sybase to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM607) Updated UCM 13.9 for iSeries to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM608) Updated UCM 34.1 for Network to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM609) Updated UCM 31.3a for Windows to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM610)

February 15, 2018	1.20	Anthony DeMedeiros (Manager, LaaS-TBCG) Mark Walsh (BA, Richter)	Updated UCM 13.2 for iSeries to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM614) Updated UCM 13.2 for Windows/*nix to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM615) Updated UCM 13.2 for Oracle to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM616) Updated UCM 13.2 for SQL to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM617)
February 20, 2018	1.21	Anthony DeMedeiros (Manager, LaaS-TBCG) Mark Walsh (BA, Richter)	Updated UCM 13.6 for iSeries to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM619) Updated UCM 13.9 for Applications to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM620) Updated UCM 12.1 for VMWare ESXi to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM625) Updated UCM 12.2 for VMWare ESXi to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM626) Updated UCM 31.2 for SQL to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM628)
March 1, 2018	1.22	Mark Walsh (BA, Richter)	Updated UCMs 13.1, 13.2, 13.7, 13.8, 13.10, 13.12, and 31.5 to include Tandem and include actions to be taken by Log Reviewers
March 1, 2018	1.22	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM 13.5 to reflect Decommissioning of UCM for Oracle Databases. Use Case Status provides rationale

March 22, 2018	1.23	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM 13.2 for Windows and *nix to reflect change of exception report to alert. Updated Required Output, Recipient(s), Actions Performed, and Retention of triage/follow up/resolution sections for each UCM - (Reference CRUCM674 & CRUCM675)
May 3, 2018	1.24	Anthony DeMedeiros (Manager, LaaS-TBCG)	Added new use case, UCM 25.3e, for ESXi devices. Logic permits that as long as the VMWare host is still sending at least one ESXi sourcetype it will not trigger a UCM 25 alert. If no ESXi sourcetypes report within 24 hours, a Remedy incident will be generated for that host.
May 23, 2018	1.25	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM 13.15 for all flavours to reflect additional criteria for the “Anomalies to follow up/investigate” section, specifically “If the column “Dest_User_Privileged” has no data or is showing”0” then check Active Directory to identify if the ID is Privileged. If the ID is <u>not</u> Privileged then it should be considered an EOI.”
June 5, 2018	1.26	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated the Use Case Sanity Validation section of all use cases with enhanced verbiage on coverage of validation testing.
June 5, 2018	1.26	Anthony DeMedeiros (Manager, LaaS-TBCG)	Updated UCM 13.9 Fire ID to include logic related to CyberArk and Fire ID usage in a 24 hour period.
August 20, 2018	1.27	Mark Walsh (BA, Richter)	Updated UCMs 12.1, 12.2, 13.2, 13.14a, 13.15, 31.2, 31.3, and 34.1 to include VBOS and include actions to be taken by Log Reviewers
August 20, 2018	1.27	Mark Walsh (BA, Richter)	Updated UCMs 13.2, 31.3, and 31.5 for VMWare to include Vcentre and include actions to be taken by Log Reviewers
August 20, 2018	1.27	Mark Walsh (BA, Richter)	Updated UCMs 12.1, 12.2, 13.3, 13.4, 13.7, 13.12, 13.14a, 31.2, 31.3, 31.5, and 34.1 to include Middleware (RSA AM, Netezza) and include actions to be taken by Log Reviewers

Document Owner(s):

The primary contact(s) for questions regarding this document is:

Name: Christine Dewhurst
Title: Director and Head of Technology Business Control Group
Phone: (416) 502-4724
Email: christine.dewhurst@bmo.com

Review and Approval:

Date	Approved Yes or No with comments	Name	Title	Group
June 26, 2017	Approved	Christine Dewhurst	Director and Head	Technology Business Controls Group
October 3, 2017	Approved	Christine Dewhurst	Director and Head	Technology Business Controls Group
October 4, 2017	Approved	Christine Dewhurst	Director and Head	Technology Business Controls Group

Proprietary Notice

This document contains confidential information that is the property of Bank of Montreal. Reproduction, utilization or disclosure of the proprietary portion of this document is prohibited.

General Notice

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

Version Control Notice

This document is a controlled issue that supersedes all previous issues. Please archive any previous copy of this document dated prior to the version and publication date noted on this page.

Table of Contents

1.0 Scope

The scope of endpoints covered by this LaaS Use Case document includes server platforms (Windows, Unix, Linux flavours, VMware, iSeries, Mainframe zOS), various network devices (including, but not limited to, switches (Cisco), firewalls (Checkpoint, Juniper, Nortel), Alteon, Raritan incident, Bluecoat, BTINS, etc.), Databases (Oracle, SQL, Sybase, PostgreSQL), and L1/L2.

2.0 Splunk LaaS Use Case Handling

The sections provide high level summaries of the Baseline Use Cases which have been defined for Splunk-LaaS, along with outlining actions to be performed by the recipients of the output (i.e. alerts, exception reports) from Splunk-LaaS.

UCM 12.1	
Use Case Title:	Multiple Failed Authentications - Multiple Users, Single Source Host, Single Destination Host
Use Case Description:	Single host authentication attempts to (single) destination using multiple accounts Greater than **20 failed authentications in a minute** by multiple users from single source host to single destination host. This covers applications, databases, VMware, network devices, mainframe and server platforms.
Context/Value:	Identify brute force attacks from single host to multiple accounts to detect unauthorized access.
Owner:	Director of CyberSecurity Ops
Use Case Review Frequency:	At least annually
Required output:	Alert strategically, in the interim it will be an exception based report. Exception Alert – iSeries, Windows/*nix, Oracle, Network, Applications, PostgreSQL, SQL, Sybase, VMWare ESXi Exception Report – VBOS, Middleware
Recipient(s):	CSOC IPC, however, in the interim it will be the Security Analyst (formerly log reviewers) Security Analyst – iSeries, Windows/*nix, Oracle, Network, Applications, PostgreSQL, SQL, Sybase, VMWare ESXi Alerts
Actions performed:	**Security Analyst (interim) – Exception Reporting:** 1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any report content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. See '**Anomalies to be followed up on**' 2. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days.

If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.

Security Analyst – Exception Alert (iSeries, Windows/*nix, Oracle, Network, Applications, PostgreSQL, SQL, Sybase, VMWare ESXi):

1. Security analyst receives the UCM 12.1 iSeries, Windows/*nix, Oracle, PostgreSQL, SQL, Sybase, Network, VMWare ESXi, and Application alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com.
2. Security analyst assesses the alert and identifies if there is an exception. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'.
   Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days.

   If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.

CSOC IPC (strategically):
Alert goes to CSOC IPC via IPC@bmo.com account that triage, follow up and resolve as per the requirements of CSOC IPC playbook.

Stakeholders (i.e. User groups, Security Analysts, COE support groups, etc.) have access to the use case output within Splunk and can leverage the output for further investigation and follow up, where required. They will be able to drill down further into details through a real-time view within Splunk.

CSOC IPC to communicate any compliance related feedback to the corresponding COE Compliance officers:

1. Elmer Valenzuela – EPS, CMRI
2. Allen Cui – NS
3. Nand Tonoo – DWS

Anomalies to be followed up on:
Applications/Databases
Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

iSeries

	Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output. **Tandem** Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output. **Mainframe** Refer to 'Mainframe Support Document v.1.3' for further details. Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output. **Network Devices:** Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Exception Reports/Alerts, logbook and any analysis performed on the reports should be retained for a period of at least 24 months (as per IMRR RRS – 1ADM25). Exception Alerts (iSeries, Windows/*nix, Oracle, PostgreSQL, SQL, Sybase, Network, Application, VMWare ESXi) goes to Security Analyst via the LaaS Exception Reporting mailbox. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Alert (strategically) goes to CSOC IPC via ipc@bmo.com that triage, follow up and resolve as per the requirements of CSOC IPC playbook. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Use Case Status:	Approved on 12/07/2016 by Louise Dandonneau (Windows, Unix, Linux, Cisco, Juniper) Approved on 06/29/2017 by Anthony DeMedeiros – iSeries Approved on 07/12/2017 by Anthony DeMedeiros – Mainframe applications Approved on 07/17/2017 by Anthony DeMedeiros – Mainframe zOS Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/18/2017 by Anthony DeMedeiros – Network devices Approved on 07/20/2017 by Anthony DeMedeiros – Sybase Approved on 07/24/2017 by Anthony DeMedeiros – IDS (Siteprotector) Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe databases Approved on 05/12/2017 by Christine Dewhurst – ORACLE Approved on 05/12/2017 by Christine Dewhurst – MSSQL Approved on 07/31/2017 by Anthony DeMedeiros – PostgreSQL Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi Approved on 01/29/2018 by Anthony DeMedeiros – Tandem

Next Review Date:	December 31, 2018
Review Date Status:	Approved on 01/19/2018 by Vicky Laurens

UCM 12.2	
Use Case Title:	Multiple Failed Authentications - Single User, Single Source Host, Multiple Destination Hosts
Use Case Description:	Greater than **20 failed authentications in a minute** by a single user from a single source host to multiple destination hosts. This covers applications, VMware, databases, mainframe, iSeries, network devices and server platforms.
Context/Value:	Identify brute force attacks from single host to multiple accounts to detect unauthorized access.
Owner:	Director of CyberSecurity Ops
Use Case Review Frequency:	At least annually
Required output:	Alert strategically, in the interim it will be an exception based report. Exception Alert – iSeries, Applications, PostgreSQL, MSSQL, Oracle, Sybase, VMWare ESXi Exception Report – VBOS, Middleware
Recipient(s):	CSOC IPC, however, in the interim it will be the Security Analyst (formerly log reviewers) Security Analyst – iSeries, Applications, PostgreSQL, MSSQL, Oracle, Sybase, VMWare ESXi Alert
Actions performed:	**Security Analyst – Exception Report (interim):** 1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any report content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. See '**Anomalies to be followed up on**' 2. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. **Security Analyst – Exception Alert (iSeries, Applications, PostgreSQL, MSSQL, Oracle, Sybase, VMWare ESXi):** 1. Security analyst receives the UCM 12.2 iSeries, PostgreSQL, MSSQL, Oracle, Sybase, Application, and VMWare ESXi alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied

(i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high ‘event count’ may be an operational issue that further needs to be followed up with the operational support teams and not considered ‘security related’.
Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user’s manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days.

If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.

CSOC IPC (strategically):
Alert goes to CSOC IPC via IPC@bmo.com account that triage, follow up and resolve as per the requirements of CSOC IPC playbook. Evidence of tracking, following up and resolution must be retained for at least a 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.

Stakeholders (i.e. User groups, Security Analysts, COE support groups, etc.) have access to the use case output within Splunk and can leverage the output for further investigation and follow up, where required. They will be able to drill down further into details through a real-time view within Splunk.
Alert goes to CSOC IPC who triage, follow up and resolve as per the requirements of CSOC IPC playbook.

CSOC IPC to communicate any compliance related feedback to the corresponding COE Compliance officers:

1. Elmer Valenzuela – EPS, CMRI
2. Allen Cui – NS
3. Nand Tonoo – DWS

Anomalies to be followed up on:
Applications/Databases
Security Analysts to follow up with user’s manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

iSeries
Security Analysts to follow up with user’s manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

Tandem
Security Analysts to follow up with user’s manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

Mainframe:
Refer to ‘Mainframe Support Document v.1.3’ for further details. Security Analysts to follow up with user’s manager/account owner for any personal/generic IDs reported on.

	Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output. **Network devices:** Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Exception reports (alerts), logbook and any analysis performed on the reports should be retained for a period of at least 24 months (as per IMRR RRS – 1ADM25). Exception Alerts (iSeries, Applications, PostgreSQL, MSSQL, Oracle, Sybase, and VMWare ESXi) goes to Security Analyst via the LaaS Exception Reporting mailbox. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Alert goes to CSOC IPC via ipc@bmo.com that triage, follow up and resolve as per the requirements of CSOC IPC playbook. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Use Case Status:	Approved on 12/07/2016 by Louise Dandonneau Approved on 06/29/2017 by Anthony DeMedeiros – iSeries Approved on 07/12/2017 by Anthony DeMedeiros – Mainframe applications Approved on 07/17/2017 by Anthony DeMedeiros – Mainframe zOS Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/18/2017 by Anthony DeMedeiros – Network devices Approved on 07/20/2017 by Anthony DeMedeiros – Sybase Approved on 07/24/2017 by Anthony DeMedeiros – IDS (Siteprotector) Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe databases Approved on 05/12/2017 by Christine Dewhurst – ORACLE Approved on 05/12/2017 by Christine Dewhurst – MSSQL Approved on 07/31/2017 by Anthony DeMedeiros – PostgreSQL Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi Approved on 01/29/2018 by Anthony DeMedeiros – Tandem
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 01/19/2018 by Vicky Laurens

UCM 13.1	
Use Case Title:	Audit policy changes – Windows Audit policy changes – Linux Audit policy changes – AIX Audit policy changes – HPUX Audit policy changes – Solaris Audit logging changes – Cisco Audit logging changes – iSeries Audit logging changes - Tandem Audit logging changes – Applications Audit logging changes – Network Devices Audit logging changes – VMware
Use Case Description:	**Cisco, Solaris, Bluecoat, iSeries, Tandem:** Exception based report on audit configuration changes for Bluecoat, Cisco IOS, Nexus, ACS, iSeries and Solaris prioritizing first critical, regulatory identified assets (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity). **Windows, Linux, HPUX, AIX, Applications:** Alert/Exception based report on audit policy/audit configuration logging changes for Windows, Unix, Linux, various Applications prioritizing first critical, regulatory identified assets (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity).
Context/Value:	Identify initialization of audit logs that could indicate that the log function was modified or disabled by a user to hide their actions. Initialization, stopping, or pausing of the audit logs or turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	**Cisco, Solaris, Bluecoat, iSeries, Tandem:** Exception report **Windows, Linux, HPUX, AIX, Applications:** Exception Report (Alert) goes to Security Analysts (formerly Log Reviewers)
Recipient(s):	**Cisco, Solaris, Bluecoat, iSeries, Tandem:** Security Analysts (formerly Log Reviewers) **Windows, Linux, HPUX, AIX, Applications:** Security Analysts (formerly Log Reviewers)
Actions performed:	**Cisco/Solaris/iSeries/Tandem:** 1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up (‘See **Anomalies to be followed up on’**) and create a Remedy ticket and assigns to the appropriate Remedy support queue. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user’s manager or other supporting group(s) as necessary. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all

details of the exception provided to them for further follow up.

Anomalies to be followed up on:
Cisco:
Any change performed outside of the network support personnel should be followed up on OR where In_AD=0 and In_ITIM=0 (which indicates that the user ID doesn't existing in either Active Directory or ITIM). Security analysts should also refer to the endpoint logging configuration for Cisco IOS, Nexus and ACS to identify any specific change by an authorized network support team member/account/ID that would deviate from the standard endpoint logging configuration. In addition, any generic account/ID making changes without proper traceability should also be further investigated and correlated back to an authorized change record.

Solaris:
Any entries in the report need to be investigated further with the COE support team by requesting them to provide the output from 'ls lrt' on the audit config file (i.e. audit_control). This should show the date/timestamp of when this file was last modified. If the file was modified within the last 24 hrs. this indicates that someone made a change to the audit logging configuration file. If the date/timestamp is > 24 hrs. then no change was made to the audit logging configuration file and the investigation can be closed.

iSeries:
Any entries in the report need to be investigated to understand if there was a valid CR for the change. If no valid CR was raised, SOC Operations/60 Yonge Ops (Remedy group) should be engaged to understand why the change was made and/or follow up with user's manager if a personal ID was used to make the change.

Tandem:
Any entries in the report need to be investigated to understand if there was a valid CR for the change. If no valid CR was raised, SSTS (Remedy group) should be engaged to understand why the change was made and/or follow up with user's manager if a personal ID was used to make the change.

Applications:
Any entries in the report need to be investigated to understand if there was a valid CR for the change. If no valid CR was raised, Security Analyst should engage the appropriate application support team to understand why the change was made and/or follow up with user's manager if a personal ID was used to make the change.

Network Devices:
Any entries in the report need to be investigated to understand if there was a valid CR for the change. If no valid CR was raised, the endpoint owner should be engaged to understand why the change was made and/or follow up with user's manager if a personal ID was used to make the change.

Windows, Linux, HPUX, AIX, Applications:

1. Security analyst receives the UCM 13.1 Audit Policy Changes exception report (alert) to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com.
2. Security analyst creates a **Remedy ticket** and assigns it to the corresponding support team for follow up and investigation. The Security Analyst may engage CSOC IPC as necessary if they detect suspicious activity. A **logbook entry** is created for tracking of the alert. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the

	2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **NOTE**: HPUX endpoints are not onboarded to Centrify due to a technical limitation (Centrify supports HPUX for non-trusted systems; but BMO is trusted. HPUX has its own security controls which are more stringent than other standard Unix flavours). Since authentication is achieved locally for HPUX (and not via Centrify), the source information may be missing, however, **destination information** will be populated only in the Splunk output i.e. alert that will show activities performed on the destination host. In this case the source and destination are the same.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	**Cisco/Solaris/iSeries/Tandem/Bluecoat/network devices:** Exception reports, logbook and any analysis performed on the reports should be retained for a period of at least 24 months (as per IMRR RRS – 1ADM25). **Windows, Linux, HPUX, AIX, Applications:** Exception Report (Alert) goes to Security Analyst via the LaaS Exception Reporting mailbox. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Use Case Status:	Approved on 01/10/2017 by Vicky Laurens – Windows Approved on 02/06/2017 by Vicky Laurens - Linux Approved on 02/21/2017 by Vicky Laurens – HPUX Approved on 05/11/2017 by Christine Dewhurst – Solaris Approved on 05/08/2017 by Vicky Laurens - AIX Approved on 04/24/2017 by Christine Dewhurst – Cisco Approved on 06/28/2017 by Anthony DeMedeiros – iSeries Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/28/2017 by Anthony DeMedeiros – Network Devices Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi Approved on 07/17/2017 by Anthony DeMedeiros - Applications
Next Review Date:	January 31, 2019
Review Date Status:	Approved on 02/08/2018 by Anthony DeMedeiros

UCM 13.2	
Use Case Title:	Disable Logging/Logging disablement – Windows Disable Logging/Logging disablement – Linux Disable Logging/Logging disablement – HPUX Disable logging/logging disablement – Cisco Disable logging/logging disablement – Solaris Disable logging/logging disablement – AIX Disable logging/logging disablement – iSeries Disable logging/logging disablement - Tandem Disable logging/logging disablement – Bluecoat Disable logging/logging disablement – Databases (Oracle) Disable logging/logging disablement – Databases (MS SQL) Disable logging/logging disablement – network devices Disable logging/logging disablement – Applications Disable logging/logging disablement – VBOS Disable logging/logging disablement - VMWare
Use Case Description:	Alert/Report on **Windows** system shutdowns and restarts as an indication that someone tried to shut down the Log Service to cover his or her activity. Please note that the 13.2 Windows report is not required to be reviewed daily. It can be used to for further investigation by the Security analysts for UCM 13.1 and UCM 25. **Rationale for not making 13.2 Windows a report that gets reviewed daily:** 1) Event 1100 is often a prelude to system shutdown. It may also stop and restart in a short time period 2) If the logging service shutdown was a result of a persistent issue then UCM 25.X will trigger 3) An intentional logging shutdown is often accomplished by modifying the audit policies. This scenario gets caught by the audit policy change UCM • Exception Alert/Report on logging disablement on iSeries • Exception Alert/Report on logging disablement on Bluecoat Devices • Exception Alert/Report on logging disablement for Databases (Oracle) • Exception Alert/Report on logging disablement for Databases (MS SQL) • Exception Alert/Report on logging disablement for Network Devices • Exception Alert/Report on user/account ID disables logging for Linux (stop audit daemon), Unix (stop audit daemon) and Network device types/flavours (**Cisco**) prioritizing first critical, regulatory identified assets • Exception Alert/Report on logging disablement on VBOS • Exception Alert/Report on logging disablement on VMWare
Context/Value:	Identify initialization of audit logs that could indicate that the log function was disabled by a user to hide their actions. Initialization, stopping, or pausing of the audit logs or turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.
Owner:	Director and Head of Technology Business Controls Group (alerts & exception reports)
Use Case Review Frequency:	At least annually.
Required output:	Exception Alert/Report goes to Security Analyst
Recipient(s):	Security Analysts (formerly Log Reviewers)
Actions performed:	**Exception Alerts/Reports:** **iSeries/Tandem:** 1. Security analyst receives a UCM 13.2 Logging Disablement exception alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. Identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution.

2. The Security analyst opens UCM 13.2 Logging disablement report and identifies any changes to logging levels that would indicate a disablement of logging on the iSeries. See '**Anomalies to be followed up on'** below. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days.

   If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.

Windows:

1. Security analyst receives a UCM 13.2 Logging Disablement exception alert to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. Identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution.
2. The Security analyst opens UCM 13.2 Logging disablement – Windows report and identifies list of all endpoints that have been shut down/restarted in the last 24 hrs.
3. Correlate data between UCM 25 for critical and non-critical endpoints. If there are common endpoints in UCM 13.2 and UCM 25, these endpoints should be further investigated as this indicates that due to some activity on this endpoint, the endpoint has stopped logging. If no common endpoints between the two reports, move to b).
4. Leverage UCM 13.1 Audit policy changes for Windows to identify any endpoints that may be common between UCM 13.1 and UCM 13.2, this may indicate a malicious user has made/or attempting to update the way the system logs and is attempting to shutdown the logging services on the endpoint to hide their actions. The common endpoints identified need to be further investigated. If no common endpoints between the two reports, move to c).
5. Drill down further into 13.2 Windows events in the Splunk online report or perform a search on the endpoint in question and look at events leading up to event code 1100 and after which provides some insight as to why the endpoint may have been shutdown i.e. patch applied etc.
   Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days.

   If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.

Anomalies to be followed up on (iSeries):

TSV0001 'change to system values', 'QAUDCTL' and 'QAUDLVL', 'QAUDLVL2' need to be evaluated with the iSeries support team.

	Anomalies to be followed up on (Databases): Security analysts should follow up with database support teams on any disabled logging events in the exception report immediately. Further production trending on the report is required to develop a baseline and detect further anomalies. Security analysts should engage ISO/Compliance officers/endpoint owners accordingly. **Anomalies to be followed up on (Applications):** Security analysts should follow up with the appropriate application support teams on any disabled logging events in the exception report immediately. Further production trending on the report is required to develop a baseline and detect further anomalies. Security analysts should engage ISO/Compliance officers/endpoint owners accordingly. **Anomalies to be followed up on:** Any change where the ID used to make the change is In_AD=0 or In_ITIM=0. Further production trending on the report is required to develop a baseline and detect further anomalies. Security analysts should engage ISO/Compliance officers/endpoint owners accordingly. **Exception Alert (*nix, Network, Oracle, SQL):** 1. Security analyst receives a UCM 13.2 Logging Disablement exception alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst creates a **Remedy ticket** and assigns it to the corresponding support team for follow up and investigation. The Security Analyst may engage CSOC IPC as necessary if they detect suspicious activity. A **logbook entry** is created for tracking of the alert. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Exception Alerts/Reports go to Security Analyst via the LaaS Exception Reporting mailbox. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Use Case Status:	Approved on 04/03/2017 by Christine Dewhurst – Windows Approved on 05/03/2017 by Vicky Laurens - Unix (AIX and Solaris) Approved on 04/06/2017 by Vicky Laurens - Unix – HPUX Approved on 03/15/2017 by Vicky Laurens - Linux Approved on 02/17/2017 by Christine Dewhurst – Cisco Approved on 02/27/2017 by Vicky Laurens - Cisco Approved on 07/11/2017 by Anthony DeMedeiros - iSeries Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/19/2017 by Anthony DeMedeiros – Databases (Oracle)

	Approved on 07/28/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 07/31/2017 by Anthony DeMedeiros - Networks
Next Review Date:	February 28, 2019
Review Date Status:	Approved on 03/01/2018 by Anthony DeMedeiros

UCM 13.3	
Use Case Title:	Authentication (Success/Failure) Activity Dashboard
Use Case Description:	Authentication activity (Successful and failure) dashboard by ID for Windows, VMware, Unix, Middleware, iSeries, Tandem, Mainframe, Network device types/flavours (like Cisco, Juniper, Bluecoat, etc.), applications and databases prioritizing first critical, regulatory identified assets. Authentication activity (Successful and failure) dashboard by ID for applications and databases.
Context/Value:	Identify unauthorized access to BMO devices. To identify a security breach/operational issue due to the activity is occurring often/high volume event. This dashboard can be used to identify terminated bank employees that may still be accessing BMO systems after their termination date.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Dashboard
Recipient(s):	Security analysts (primary users), CSOC IPC, User Managers
Actions that can be performed:	This dashboard can be used to perform the following, but not limited to: • Single pane view of all servers/network devices/applications/databases a user may have logged into over a specific time period • Top 10 view of the endpoints a particular user has logged into over a specific time period • Successful logins to a server/network device/application/database • Failed logins to a server/network device/application/database • Preliminary understanding of user activity i.e. users that login after terminated date
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Extracts i.e. reports can be exported from Splunk to support investigations, where required and should follow BMO standards on retention.
Use Case Status:	Approved on 05/12/2017 by Christine Dewhurst – Platforms (Windows, Unix/Linux, Cisco) Approved on 05/31/2017 by Anthony DeMedeiros – Applications and Databases (Oracle) Approved on 06/30/2017 by Anthony DeMedeiros – iSeries Approved on 07/12/2017 by Anthony DeMedeiros - Bluecoat Approved on 07/12/2017 by Anthony DeMedeiros – Mainframe applications Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe zOS Approved on 07/24/2017 by Anthony DeMedeiros – Databases (Sybase) Approved on 07/26/2017 by Anthony DeMedeiros – Databases (Oracle) Approved on 07/26/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 07/27/2017 by Anthony DeMedeiros - Checkpoint Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe Databases Approved on 07/28/2017 by Anthony DeMedeiros - Networks Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi Approved on 01/29/2018 by Anthony DeMedeiros – Tandem

Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.4	
Use Case Title:	Logon/Logout Activity Dashboard
Use Case Description:	A login events (login/logout) dashboard for Windows, Unix, VMware, iSeries, Tandem, Network device types/flavours (like Cisco, Juniper, Bluecoat, etc.), Middleware, applications and databases prioritizing first critical, regulatory identified assets.
Context/Value:	Identify unauthorized access to BMO devices. This dashboard can be used to identify terminated bank employees that may still be accessing BMO systems after their termination date.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Dashboard
Recipient(s):	Security analysts (primary users), CSOC IPC, User Managers
Actions that can be performed:	This dashboard can be used to perform the following, but not limited to: • Login/logout activity for users for a specific time range • Top 10 view of the endpoints a particular user has logged into/logged out of over a specific time period • Understand whether a user has logged in after termination date
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Extracts i.e. reports can be exported from Splunk to support investigations, where required and should follow BMO standards on retention.
Use Case Status:	Approved on 05/12/2017 by Christine Dewhurst Approved on 07/12/2017 by Anthony DeMedeiros - Bluecoat Approved on 07/12/2017 by Anthony DeMedeiros - iSeries Approved on 07/26/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 07/26/2017 by Anthony DeMedeiros – Databases (Oracle) Approved on 07/31/2017 by Anthony DeMedeiros - Databases (Sybase) Approved on 07/27/2017 by Anthony DeMedeiros - Checkpoint Approved on 07/28/2017 by Anthony DeMedeiros - Networks Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi Approved on 01/29/2018 by Anthony DeMedeiros – Tandem
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.5/UCM 13.5c	
Use Case Title:	System Utility Usage by User UCM 13.5 – Windows UCM 13.5 - *nix UCM 13.5 - Oracle
Use Case Description:	Exception based report on use of system utilities by ID for Windows, Unix prioritizing first critical, regulatory identified assets (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity). **Windows utilities being captured:** • regedit.exe • FTP.exe • msconfig.exe • powershell.exe • MRT.exe **Unix/Linux utilities being captured:**: • chgrp • chown • chmod • kill • mv • rcp • rlogin • rsh • telnet • tft
Context/Value:	Identify unauthorized use and unauthorized configuration changes of systems.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report
Recipient(s):	Security analysts (formerly log reviewers),
Actions that can be performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (see '**Anomalies to be followed up on**' below) follow the guidance below. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.

	Anomalies to be followed upon: • Security analysts are to develop a whitelist of system utilities and trend the report over time to help identify system utility exceptions. Whitelist opportunities identified by the security analysts should be documented and reviewed on a regular basis with the use case owner/compliance officer and ISOs for review and approval to help fine-tune the use case. Approved whitelists entries should be incorporated into the use case as fine-tuning opportunities at the discretion of the use case owner. • Exceptions/anomalies identified as a result of 'whitelisting' should be followed up and investigated with the support teams and/or user manager accordingly. • In_AD or In_ITIM=0 entries should be followed up on and investigated for usage of system utilities as a priority.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy Incident Management process and the priority assigned to ticket.
Use Case Status:	Approved on 06/16/2017 by Anthony DeMedeiros DECOMMISSIONED on 03/01/2018 via CRUCM638 and approved by Anthony DeMedeiros for Oracle Databases. The rationale is that based on feedback from the DBAs, the existing logging configurations for Oracle does not provide the necessary information to the Log Reviewers in order to action events in this report. As such, it is recommended that this report be removed from being sent to the Log Reviewers to be actioned until the logging configurations are set to capture the necessary information (if ever). For the reason above, UCM 13.5 for Oracle Databases is no longer required.
Next Review Date:	June 30, 2019
Review Date Status:	Approved on 07/03/2018 by Anthony DeMedeiros

UCM 13.6	
Use Case Title:	Report on the use of non-compliant (risky) protocols/unauthorized services such as ftp, telnet, rlogin, etc.
Use Case Description:	Exception based report/alert on the use of non-compliant (risky) protocols/unauthorized services such as ftp, telnet, rlogin, etc. for open systems, network devices, and iSeries.
Context/Value:	Identify the use of risky protocols that provide information in clear text such as passwords, provide detailed network information that can be used by hackers to gain knowledge about systems, etc. ISM states: IS 06.02.3 - Ports, services, and similar facilities installed on a computer or network facility which is not specifically required for business functionality shall be disabled or removed.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Reports: ◦ 13.6 – Use of Non-Compliant Protocols or Services - All ◦ 13.6a - Use of Non-Compliant Protocols or Services - Internal to External Exception Alerts (iSeries)
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions (report/alert) that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (see '**Anomalies to be followed up on**' below) follow the guidance below. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Log Reviewer Focus:** i. Log Reviewers are to prioritize their review based on the high risk scenario of use of Non-Compliant Protocols or Services - Internal to External, as reported in the UCM 13.6a report. ii. Log Reviewers are to also review the UCM 13.6 report as this provides a comprehensive view of all use of Non-Compliant Protocols or Services. **Anomalies to be followed upon:** • Identify any ftp, telnet and rlogin connections that may be externally facing and follow up on these immediately (where the destination information in the report does not correspond to BMO systems or NOT in HPAM). Consult COE support teams or SOC Operations/60 Yonge Ops (Remedy group for iSeries) for business rationale

	and any open exceptions (IRIs) and Compliance/Information Security officers for corrective action, where appropriate. • For any users/accounts identified using a non-compliant protocol, consult a Compliance/Information Security officer to ensure no exemptions have been raised for the use of these services. Follow up with the user's manager/account owner to understand the uses for the non-compliant/risky protocol i.e. ftp, telnet, rlogin and document accordingly. Based upon feedback from Compliance/information security officer, corrective action should be taken. • Trend ftp, telnet, rlogin if identified for both BMO systems/Not in HPAM AND non-BMO systems and investigate accordingly with the identified COE support teams and engage the compliance officers/ISOs accordingly on whether further corrective action needs to be taken. Fine-tune the use case accordingly based on further investigations and consult Compliance officers and ISOs, where appropriate. **Network Devices:** Any network device owned by NS (Network Services) should not allow any ftp/telnet connections and should be followed up immediately. Network devices (for example CMRI) may have valid exceptions raised and ISOs should be engaged accordingly. Whitelists should be drafted by the log reviewers and maintained leveraging the confirmed ISO exceptions.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports/alerts along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy Incident Management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 06/02/2017 by Anthony DeMedeiros Approved on 07/31/2017 by Anthony DeMedeiros – Networks Approved on 07/21/2017 by Anthony DeMedeiros - iSeries
Next Review Date:	June 30, 2019
Review Date Status:	Approved on 07/03/2018 by Anthony DeMedeiros

UCM 13.7	
Use Case Title:	System startups/shutdown activity – applications/databases/VMWare/Middleware
Use Case Description:	Exception report for application/process (security or audit)/services start-ups, shutdowns, failures and re-starts and other unusual system activities for applications/databases.
Context/Value:	Identify any unauthorized activity that would impact the availability of a critical system.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (see '**Anomalies to be followed up on**' below) follow the guidance below. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed upon (applications/databases/VMWare):** • Identify any unusual application/database/VMware system/start up/shutdown activity and engage the application/database/VMware support team to aid in identifying any anomalies. For example, system shutdowns during business hours are 'unusual' as most shut downs/restarts would typically be planned during non-business hours/after business hours/period of low activity. Security analysts should develop a whitelist/baseline to help in fine-tuning the use case.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy Incident Management process and the priority assigned to ticket.
Use Case Status:	Approved on 07/17/2017 by Anthony DeMedeiros - Applications

	Approved on 07/26/2017 by Anthony DeMedeiros – Databases (Oracle) Approved on 07/24/2017 by Anthony DeMedeiros – Databases (Sybase) Approved on 07/26/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 07/31/2017 by Anthony DeMedeiros – PostgreSQL Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 13.7	
Use Case Title:	Privileged Authentication Activity by System Process Dashboard
Use Case Description:	Dashboard for system/process(security or audit)/services start-ups, shutdowns, failures and re-starts and other unusual system activities for Windows, Unix and Network device types/flavours prioritizing first critical, regulatory identified assets
Context/Value:	Identify any unauthorized activity that would impact the availability of a critical system.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Dashboard
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	This dashboard can be used to perform the following, but not limited to: • Single pane view of all servers/network devices and privileged authentication activity by system process over a specific time period • Identify any trends in system process activity that may be questionable/malicious • Develop whitelists • Supports identifying potential malware
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Use Case Status:	Approved on 06/16/2017 by Anthony DeMedeiros
Next Review Date:	June 30, 2019
Review Date Status:	Approved on 07/03/2018 by Anthony DeMedeiros

UCM 13.7	
Use Case Title:	Privileged Authentication Activity by System Process (iSeries)
Use Case Description:	Report on iSeries system process activity (event codes : CPF111C , CPF111D, , CPI2283, CPI2284, TST001 ‘use of service tools’, TCD0003)
Context/Value:	Identify any unauthorized activity that would impact the availability of a critical system.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (see ‘**Anomalies to be followed up on**’ below) follow the guidance below. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user’s manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed upon:** The appearance of an unknown system-level object will need to be researched or verified with the Information Security Officer (ISO) to determine appropriateness of the privileged activity. In the absence of a whitelist of system objects/processes on various platforms, the Security Analyst needs to draft a whitelist and perform baselining on production data to help them to identify additional anomalies moving forward. Compliance and Information Security officers should be engaged/consulted accordingly for any suspected anomalies to the baseline to obtain concurrence.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS –

	1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Use Case Status:	Approved on 07/11/2017 by Anthony DeMedeiros
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 13.7	
Use Case Title:	Privileged Authentication Activity by System Process (Tandem)
Use Case Description:	Report on Tandem system process activity
Context/Value:	Identify any unauthorized activity that would impact the availability of a critical system.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	4. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 5. For any identified exceptions (see '**Anomalies to be followed up on**' below) follow the guidance below. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 6. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed upon:** The appearance of an unknown system-level object will need to be researched or verified with the Information Security Officer (ISO) to determine appropriateness of the privileged activity. In the absence of a whitelist of system objects/processes on various platforms, the Security Analyst needs to draft a whitelist and perform baselining on production data to help them to identify additional anomalies moving forward. Compliance and Information Security officers should be engaged/consulted accordingly for any suspected anomalies to the baseline to obtain concurrence.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy

	incident management process and the priority assigned to ticket.
Use Case Status:	Approved on 07/11/2017 by Anthony DeMedeiros
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 13.8	
Use Case Title:	Windows System Level Object Changes (modifications/deletions) Unix/Linux system level object changes (modifications/deletions) iSeries system level object changes (modifications/deletions) Tandem system level object changes (modifications/deletions) Network Device System Level Object Changes (modification/deletions) Database object changes - Oracle
Use Case Description:	Exception based report focusing on \Windows\System32 folder on modifications/deletions of system level objects/files. Exception based report focusing on /etc/bin directory system file modifications/deletions – Unix/Linux. Exception based report focusing on system object modifications/deletions Exception based report focusing on deletion of LIB commands on Q* libraries - TDO0001 and change authorization and object authority on QLIB* (TCA0001) and event code: TAD0021. Exception based report focusing on database object changes - Oracle.
Context/Value:	Identify unauthorized modification / deletion of system level objects.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See '**Anomalies to be followed up on**' below), the security analyst is responsible for following up accordingly. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed up on:** **Windows** There are certain critical system-level objects in the Windows system 32 folder that are critical towards maintaining the security and availability of the target system. The Security Analyst has to analyze the usage of these system-level objects to determine the appropriateness of the privileged activity. For example, a user launching allowed utilities like cmd.exe or net.exe would be appropriate for an authorized system administrator. The use of these utilities would be well within the norm of day to day operations. On the other hand, modifying the registry and/or SAM (system access management) files would be an Event of Interest (EOI) because this action could change the security posture of the

	target system (i.e. 4657 A registry value was modified, 4660 An object was deleted) are some key events to investigate further. Furthermore, the appearance of an unknown system-level object will need to be researched or verified with the Information Security Officer (ISO) to determine appropriateness of the privileged activity. **Unix/Linux/Databases** There are certain critical system/database-level objects in the Unix/Linux directory that are critical towards maintaining the security and availability of the target system. The Security Analyst has to analyze the usage of these system-level objects to determine the appropriateness of the privileged activity. For example, a user launching allowed utilities would be appropriate for an authorized system administrator. The use of these utilities would be well within the norm of day to day operations. On the other hand, modifying the specific system files by a party outside of a system administrative group would be an Event of Interest (EOI) because this action could change the security posture of the target system are some key events to investigate further. **Network devices** Any changes made by users/accounts where In_AD=0 or In_ITIM=0 should be followed up on immediately or changes made by any users/accounts outside of the network support team should be investigated. **Tandem:** Security analysts to focus on identifying any deletion/modification of objects and follow up with the user's manager/account owner where these situations occur. **iSeries:** Security analysts to focus on identifying any deletion of LIB commands on Q* libraries - TDO0001 and change authorization and object authority on QLIB* (TCA0001) and activities on event code TAD0021 and following up user's managers/account owners where these situations occur. Furthermore, the appearance of an unknown system-level object will need to be researched or verified with the Information Security Officer (ISO) to determine appropriateness of the privileged activity. In the absence of a whitelist of system files/processes on various platforms, the Security Analyst needs to draft whitelists and perform baselining on production data to help them to identify additional anomalies moving forward. Compliance and Information Security officers should be engaged/consulted accordingly for any suspected anomalies to the baseline to obtain concurrence.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The Splunk reports are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any discrepancies of activity must be retained for at least 24 months (as per IMRR RRS –

	1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/01/2017 by Christine Dewhurst - Windows Approved on 06/23/2017 by Anthony DeMedeiros – Unix/Linux Approved on 07/17/2017 by Anthony DeMedeiros Approved on 07/27/2017 by Anthony DeMedeiros – Checkpoint
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.8b	
Use Case Title:	Access to Windows System Level Objects
Use Case Description:	Exception based report focusing on \Windows\System32 folder on access to system level objects/files.
Context/Value:	Identify unauthorized access to system level objects.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See '**Anomalies to be followed up on**' below), the security analyst is responsible for following up accordingly. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed up on:** For any cases where In_AD or In_ITIM equals 0 (meaning the ID in question is not in Active Directory or ITIM (User ID Book of Record)), then the ID who accessed the system object should be further investigated. Furthermore, the appearance of an unknown system-level object will need to be researched or verified with the Information Security Officer (ISO) to determine appropriateness of the privileged activity.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The Splunk reports are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any discrepancies of activity must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/01/2017 by Christine Dewhurst
Next Review Date:	May 31, 2019

Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.9	
Use Case Title:	Fire ID Activity Report
Use Case Description:	Exception Based Alert on Fire ID activity on iSeries, Windows, and Applications prioritizing first critical, regulatory identified assets.
Context/Value:	Identify unauthorized use of Fire ID usage (typically used by development teams when access to production is required temporarily).
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception Alert - Applications, Windows, iSeries
Recipient(s):	Fire ID Release Management Team
Actions performed:	1. Security analyst receives a UCM 13.9 Alert to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception and/or if the ID has been on-boarded to CyberArk. For any IDs not on-boarded to CyberArk or any suspected unauthorized use of a FireID, Security Analysts should follow up on these IDs with the FireID Release Management team to confirm if the use of that FireID has been approved via the existing process. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If this requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Note:** Splunk checks for Fire IDs within CyberArk and whether it has been "Checked Out" in the last 24 hours. If the Fire ID was "Checked Out" in the last 24 hours then no results will appear in UCM 13.9. If the Fire ID is being originally used outside of CyberArk or outside of a 24 hour period after its last CyberArk use then it will appear in UCM 13.9. **Disclaimer:** At the time of use case implementation, the CyberArk project is underway to onboard all IDs including fire IDs. CyberArk is a source that has been integrated into Splunk, however, coverage of Fire IDs is not complete until the CyberArk project is complete. The fire ID sources leveraged for the initial implementation of the use case include AD, ITIM and static fire ID lists provided by the Fire ID release management team. Further tuning of this use case needs to occur to make it 'truly exception based' once the CyberArk project is complete. CyberArk logs will need to integrate into this use case to track "check-outs/check-ins" of IDs to determine if Fire IDs were used outside of the authorization window.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an

	examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The Splunk Fire ID Activity Reports/Alerts are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any discrepancies of Fire ID activity must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Fire ID process maintained by the Fire ID Release Management team in GITRM.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 11/08/2016 by Christine Dewhurst Approved on 07/14/2017 by Anthony DeMedeiros - iSeries Approved on 07/20/2017 by Anthony DeMedeiros - Applications
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 12/21/2017 by Anthony DeMedeiros

UCM 13.10	
Use Case Title:	Service ID Activity Report
Use Case Description:	Activity based report on Service ID activity (based on ITIM source)
Context/Value:	Identify unauthorized service ID usage (some service IDs have credentials capable of being used by an individual) for open systems, iSeries, Tandem, applications, network devices (such as FireEye) and databases
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Activity report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	**1.** Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. (See **'Anomalies'** below) **2.** For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. **3.** If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** Any service IDs in the report where In_AD or In_ITIM = 0 needs to be followed up on and further investigated, if unknown. In addition, any rare processes that look suspicious need to be followed up on and investigated. Security Analysts need to maintain a 'whitelist' of processes run by service IDs to help identify processes that appear to be suspicious. Furthermore, the appearance of an unknown service ID will need to be researched or verified with the COE support team and/or Information Security Officer (ISO) to determine appropriateness of the privileged activity. **Considerations:** The following processes are normal for most Windows servers, however, variations in the process names could indicate malware: **1. CSRSS.EXE - Client/Server Run** **2.** Its name is often used by malware to hide on systems (CSSRS.EXE, CSRSSS.EXE, etc.) **3. LSASS.EXE - Local Security Authority** • Often targeted by malware as a means to dump passwords. Also mimicked by malware to hide on a system (lass.exe, lssass.exe, lsasss.exe, etc.). **4. SVCHOST.EXE - Service Hosting Process** • Often mimicked (scvhost, svch0st, etc.)

5. Explorer.exe - AKA Windows Explorer

- This process is often targeted by malware. Malware will often times inject this process. One indication of this is if Explorer.exe is connecting out to the internet.

Checklist:

- Check the parent/child relationships of processes, if available
- Check which users names the processes are running under, if available
- Check their command line parameters for those processes that use them, if available
- Check their digital signatures, if available
- Check their base priorities, if available
- Check the location they are being from, if available
- Check their spellings, if available
- Leverage memory analysis to detect hidden and/or injected process. Some malware can hide processes by unlinking them (among other ways). Memory analysis is a must these days, if available.
- When you get comfortable with everything here, dig deeper and check what modules are typically loaded for each process, if available
- Check and see if processes that should not be connecting out to the internet are not, if available
- Check process privileges, if available
- If wscript.exe process is running check the command line of what it is running, if available
- Investigate processes running inside %temp%, root of %appdata%, %localappdata%, recycle bin, etc. , if available
- If rundll32.exe is running check its command line as well, , if available
- "Most" legitimate user applications like Adobe, Web browsers, etc. don't spawn child processes like cmd.exe. If you see this, they should be investigated.
- Core Windows processes shouldn't be communicating out to the internet. If you see communication from these processes, dig deeper. Look for suspicious URLs/IPs, check process strings, etc.

iSeries:

Identify via baseline production trending any service IDs that appear to be suspicious and follow up with the iSeries support team accordingly. Security analysts can also review the CARK#1 report for any service IDs that have been onboarded to CyberArk that do not appear in this UCM 13.10 report. For any IDs in the 13.10 report that are NOT in the CARK#1 report, Security analysts should raise to the iSeries support team to validate the ID and to recommend onboarding to CyberArk if a valid ID.

Tandem:

Identify via baseline production trending any service IDs that appear to be suspicious and follow up with the Tandem support team accordingly. Security analysts can also review the CARK#1 report for any service IDs that have been onboarded to CyberArk that do not appear in this UCM 13.10 report. For any IDs in the 13.10 report that are NOT in the CARK#1 report, Security analysts should raise to the Tandem support team to validate the ID and to recommend onboarding to CyberArk if a valid ID.

- Production trend the service IDs and draft whitelists tactically and present to the ISOs and Compliance officers for review ad-hoc or within the CLM Splunk Log review forums accordingly. Fine-tune the use case accordingly based on further investigations and consult Compliance officers and ISOs, where appropriate. Strategically, other correlation sources i.e. Carbon Black should be leveraged as integration sources and intelligence gathered to define whitelists accordingly.

Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The Service ID activity reports are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any discrepancies of service ID activity must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/30/2017 by Anthony DeMedeiros – Servers Approved on 07/18/2017 by Anthony DeMedeiros – iSeries Approved on 07/21/2017 by Anthony DeMedeiros – Databases (Oracle) Approved on 07/25/2017 by Anthony DeMedeiros - Applications Approved on 07/27/2017 by Anthony DeMedeiros - FireEye
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.10a	
Use Case Title:	Shared ID Activity Report
Use Case Description:	Activity based report on Shared ID activity (based on ITIM source)
Context/Value:	Identify unauthorized shared ID usage (some shared IDs have credentials capable of being used by an individual).
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Activity report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	**1.** Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. (See **'Anomalies'** below) **2.** For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. **3.** If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** Any shared IDs in the report where In_AD or In_ITIM = 0 needs to be followed up on and further investigated, if unknown. In addition, any rare processes that look suspicious need to be followed up on and investigated. Security Analysts need to maintain a 'whitelist' of processes run by service IDs to help identify processes that appear to be suspicious. Furthermore, the appearance of an unknown service ID will need to be researched or verified with the Information Security Officer (ISO) to determine appropriateness of the privileged activity. **Considerations:** The following processes are normal for most Windows servers, however, variations in the process names could indicate malware: **1. CSRSS.EXE - Client/Server Run** • Its name is often used by malware to hide on systems (CSSRS.EXE, CSRSSS.EXE, etc.) **2. LSASS.EXE - Local Security Authority** • Often targeted by malware as a means to dump passwords. Also mimicked by malware to hide on a system (lass.exe, lssass.exe, lsasss.exe, etc.). **3. SVCHOST.EXE - Service Hosting Process** • Often mimicked (scvhost, svch0st, etc.) **4. Explorer.exe - AKA Windows Explorer**

	• This process is often targeted by malware. Malware will often times inject this process. One indication of this is if Explorer.exe is connecting out to the internet. **Checklist:** • Check the parent/child relationships of processes, if available • Check which users names the processes are running under, if available • Check their command line parameters for those processes that use them, if available • Check their digital signatures, if available • Check their base priorities, if available • Check the location they are being from, if available • Check their spellings, if available • Leverage memory analysis to detect hidden and/or injected process. Some malware can hide processes by unlinking them (among other ways). Memory analysis is a must these days, if available. • When you get comfortable with everything here, dig deeper and check what modules are typically loaded for each process, if available • Check and see if processes that should not be connecting out to the internet are not, if available • Check process privileges, if available • If wscript.exe process is running check the command line of what it is running, if available • Investigate processes running inside %temp%, root of %appdata%, %localappdata%, recycle bin, etc. , if available • If rundll32.exe is running check its command line as well, , if available • "Most" legitimate user applications like Adobe, Web browsers, etc. don't spawn child processes like cmd.exe. If you see this, they should be investigated. • Core Windows processes shouldn't be communicating out to the internet. If you see communication from these processes, dig deeper. Look for suspicious URLs/IPs, check process strings, etc. • Production trend the service IDs and draft whitelists tactically and present to the ISOs and Compliance officers for review ad-hoc or within the CLM Splunk Log review forums accordingly. Fine-tune the use case accordingly based on further investigations and consult Compliance officers and ISOs, where appropriate. Strategically, other correlation sources i.e. Carbon Black should be leveraged as integration sources and intelligence gathered to define whitelists accordingly.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The Shared ID activity reports are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any discrepancies of Shared ID activity must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.

Use Case Status:	Approved on 05/30/2017 by Anthony DeMedeiros
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.11	
Use Case Title:	Privileged Authentication Activity Dashboard
Use Case Description:	A dashboard which is an active and inactive user list by authentication type a. VPN Users b. Active Directory Users c. Infrastructure Device Access (Firewalls, Routers, Switches, IDS)
Context/Value:	Identify unauthorized access. To identify a security breach/operational issue due to the activity is occurring often/high volume event. This report is used to identify terminated bank employees (need a list of terminated employees).
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Dashboard
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	This dashboard can be used to perform the following, but not limited to: • Single pane view of all servers/network devices and privileged authentication activity over a specific time period • Identify any trends in privileged authentication activity that may be questionable/malicious • Develop whitelists • Leverage trend data for further investigations to support other Splunk LaaS use cases
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Extracts i.e. reports can be exported from Splunk to support investigations, where required and should follow BMO standards on retention.
Use Case Status:	Approved on 06/16/2017 by Anthony DeMedeiros Approved on 07/31/2017 by Anthony DeMedeiros – Network Devices
Next Review Date:	June 30, 2019
Review Date Status:	Approved on 07/03/2018 by Anthony DeMedeiros

UCM 13.12	
Use Case Title:	Database/Application/VMWare/Middleware System/Device configuration changes
Use Case Description:	Exception report capturing system/application/database, VMWare, Middleware configuration changes on iSeries, Tandem, applications, databases, and network devices. Exception alert capturing configuration changes on Windows and *nix for config\SAM and config\SYSTEM files, as well as modifications to the etc\shadow and etc\password files.
Context/Value:	Identify unauthorized changes to system configurations.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	• Exception Report for configuration changes made on iSeries, Tandem, applications, databases, Middleware, and network devices • Exception Alert for modifications made to config\SAM and config\SYSTEM files as well as etc\shadow and etc\password files
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions/alerts that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions/alerts See '**Anomalies to be followed up on**'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception/alert requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed up on:** Any changes made to database/application/VMWARE system/device configurations where In_AD=0 and/or In_ITIM=0 should be followed up on immediately. In addition, Security Analysts should also note any changes made within business hours as changes usually occur after business hours as to not impact daily business activity. Security analysts should use their discretion in ensuring any changes made have an authorized change request for any suspicious activity and develop a whitelist or baseline of normal business activity in order to assist in identifying anomalies. Information security officers/CSOC IPC should be engaged, where appropriate, by Security analysts.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow	The original exception reports/alerts along with the evidence of the exception review (i.e.

up/resolution:	filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/17/2017 by Anthony DeMedeiros - iSeries Approved on 07/18/2017 by Anthony DeMedeiros – Applications Approved on 07/20/2017 by Anthony DeMedeiros - Databases Approved on 07/27/2017 by Anthony DeMedeiros - Windows Approved on 07/27/2017 by Anthony DeMedeiros – Linux/Unix Approved on 07/27/2017 by Anthony DeMedeiros – Network Devices Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 13.13	
Use Case Title:	Multiple failed logins per host dashboard
Use Case Description:	Dashboard showing multiple failed logins per host (network devices/servers/VMWare/platforms/applications/databases) to be leveraged as an investigative tool by log reviewers or other key stakeholders i.e. CSOC IPC
Context/Value:	Identify unauthorized access from a host based perspective to identify potential host based attacks.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Dashboard
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	This dashboard can be used to perform the following, but not limited to: • Log reviewers can trend over time to identify any spikes in failed login activity which can indicate brute force attempt attack • Other stakeholders can use it to identify any unauthorized attempts from a host based perspective
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Any investigation leveraging this dashboard as a tool should be retained including screenshots.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 06/13/2017 by Anthony DeMedeiros - Servers Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/20/2017 by Anthony DeMedeiros - Sybase Approved on 07/28/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 06/13/2017 by Anthony DeMedeiros - Oracle Approved on 07/28/2017 by Anthony DeMedeiros - Networks Approved on 07/31/2017 by Anthony DeMedeiros – PostgreSQL Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi
Next Review Date:	June 30, 2019
Review Date Status:	Approved on 07/03/2018 by Anthony DeMedeiros

UCM 13.14a	
Use Case Title:	Multiple login failures per user
Use Case Description:	Exception based report on Windows flavours, Unix flavours, VBOS, VMWare, Middleware, various Network device types/assets (such as Cisco, Juniper, Bluecoat, etc.), iSeries, Tandem, Mainframe, applications, databases per COE where the failed login is greater than 5 attempt in less than 5 minutes by a single user from a single source host or multiple source hosts to single destination host (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity) prioritizing first critical, regulatory identified assets.
Context/Value:	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password. Will satisfy both SOX and PCI requirements.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception Report Exception Alert (iSeries, PostgreSQL, Sybase)
Recipient(s):	Security Analyst(s) (formerly Log Reviewers)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions i.e. failed logins greater than 5 where AD account lockout threshold policies don't apply (user ids not a part of AD (In_AD=0 or non-AD accounts), log reviewers use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. See '**Anomalies to be followed up on**' Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Security Analyst – Exception Alert (iSeries, PostgreSQL, Sybase):** 1. Security analyst receives UCM 13.14a (iSeries, PostgreSQL, Sybase) alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception. For any

identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'.
Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days.

If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.

Anomalies to be followed up on -
Applications/Databases:
Security Analysts to follow up with user's manager/account owner/application support team for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

Mainframe:
Refer to 'Mainframe Support Document v.1.3' for further details. Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

Bluecoat:
Any failed login attempts where In_AD=0 and/or In_ITIM=0 should be followed up on immediately and any failed login > 5 login attempts should be followed up on. Security analysts should follow up with the user's manager/account owner. Information security officers/CSOC IPC should be engaged, where appropriate, by Security analysts.

Network devices:
Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on focusing on any failed login attempts where In_AD=0 and/or In_ITIM=0 should be followed up on immediately and any failed login > 5 login attempts should be followed up on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

iSeries:
Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.

	Tandem: Security Analysts to follow up with user's manager/account owner for any personal/generic IDs reported on. Security analysts should also inform operational support teams of any operational errors in order to reduce noise in the use case output.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports/alerts along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 12/06/2016 by Christine Dewhurst Approved on 06/29/2017 by Anthony DeMedeiros – iSeries Approved on 07/12/2017 by Anthony DeMedeiros – Mainframe applications Approved on 07/17/2017 by Anthony DeMedeiros – Mainframe zOS Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/18/2017 by Anthony DeMedeiros – Network devices Approved on 07/20/2017 by Anthony DeMedeiros – Sybase Approved on 07/24/2017 by Anthony DeMedeiros – IDS (Siteprotector) Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe databases Approved on 05/12/2017 by Christine Dewhurst – ORACLE Approved on 05/12/2017 by Christine Dewhurst – MSSQL Approved on 07/31/2017 by Anthony DeMedeiros – PostgreSQL Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi Approved on 01/29/2018 by Anthony DeMedeiros – Tandem
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 12/21/2017 by Anthony DeMedeiros

UCM 13.14c	
Use Case Title:	UCM 13.14c - Multiple 'su' and 'sudo' login Failures Per User - Unix and Linux
Use Case Description:	Exception based alerts on Unix (Solaris, HPUX and AIX) and Linux flavours per COE where the failed login is greater than 3 attempts in less than 5 minutes by a single (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity) prioritizing first critical, regulatory identified assets.
Context/Value:	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password. Will satisfy both SOX and PCI requirements.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception Alert
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	**1.** Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions alerts that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. (See **'Anomalies'** below) **2.** For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. **3.** If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** Any alerts identified mean that someone attempted greater than 3 attempts to su or sudo and were unsuccessful – these failed login attempts need to be followed up on and the appropriate user manager/support teams engaged for further investigation.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports/alerts along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.

Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 02/28/2017 by Christine Dewhurst
Next Review Date:	February 28, 2019
Review Date Status:	Approved on 03/01/2018 by Anthony DeMedeiros

UCM 13.15	
Use Case Title:	UCM 13.15 – Generic Privileged Activity – Applications and Databases
Use Case Description:	Activity based report on generic privileged activity for applications
Context/Value:	Identify unauthorized/unusual privileged activity that may be occurring on applications.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Activity report initially, fine-tuned, to get to an exception based report
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** For any entries where 'In_AD' or 'In_ITIM' equals 0 indicates that the activity was performed by an ID not found in Active Directory or not within the user id book of record, ITIM. These cases should be followed up on immediately. Where In_AD and In_ITIM fields equal 1, these activities are performed by users that exist in Active Directory and ITIM. If the column "Dest_User_Privileged" has no data or is showing"0" then check Active Directory to identify if the ID is Privileged. If the ID is not Privileged then it should be considered an EOI. These cases should be scanned to ensure the user performing the activity reports into an authorized support manager. Any users who do not report into a manager or where the 'Destination_user_manager' is blank should also be investigated and validated against the Employee Directory. Furthermore, the appearance of an unknown privileged activity will need to be researched or verified with the application support teams/Compliance officer and/or Information Security Officer (ISO) to determine appropriateness of the privileged activity. - Production trend the privileged activity and draft whitelists tactically and present to the ISOs and Compliance officers for review ad-hoc or within the CLM Splunk Log review forums accordingly. Fine-tune the use case accordingly based on further investigations and consult application support teams, Compliance officers and ISOs, where appropriate. Strategically, other correlation sources i.e. Carbon Black should be leveraged as integration sources and intelligence gathered to define whitelists accordingly.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such

	use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 07/28/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 07/17/2017 by Anthony DeMedeiros - Applications
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 13.15	
Use Case Title:	UCM 13.15 – Personal Privileged Activity – Windows/VMWare UCM 13.15 – Event Code 4674 Analytics Dashboard
Use Case Description:	Activity based report on personal privileged activity in Windows.
Context/Value:	Identify unauthorized privileged activity that may be occurring on Windows platforms.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Activity report to be trended to get to an exception based report
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** For any entries where 'In_AD' or 'In_ITIM' equals 0 indicates that the activity was performed by an ID not found in Active Directory or not within the user id book of record, ITIM. These cases should be followed up on immediately. Where In_AD and In_ITIM fields equal 1, these activities are performed by users that exist in Active Directory and ITIM. If the column "Dest_User_Privileged" has no data or is showing"0" then check Active Directory to identify if the ID is Privileged. If the ID is <u>not</u> Privileged then it should be considered an EOI. These cases should be scanned to ensure the user performing the activity reports into an authorized support manager. Any users who do not report into a manager or where the 'Destination_user_manager' is blank should also be investigated and validated against the Employee Directory. Furthermore, the appearance of an unknown privileged activity will need to be researched or verified with the Compliance officer and/or Information Security Officer (ISO) to determine appropriateness of the privileged activity. **Considerations:** The following processes are normal for most Windows servers, however, variations in the process names could indicate malware: **1. CSRSS.EXE - Client/Server Run** • Its name is often used by malware to hide on systems (CSSRS.EXE, CSRSSS.EXE, etc.) 2. **LSASS.EXE - Local Security Authority** • Often targeted by malware as a means to dump passwords. Also mimicked by malware to hide on a system (lass.exe, lssass.exe, lsasss.exe, etc.).

	3. **SVCHOST.EXE - Service Hosting Process** • Often mimicked (scvhost, svch0st, etc.) 4. **Explorer.exe - AKA Windows Explorer** • This process is often targeted by malware. Malware will often times inject this process. One indication of this is if Explorer.exe is connecting out to the internet. **Checklist:** • Check the parent/child relationships of processes, if available • Check which users names the processes are running under, if available • Check their command line parameters for those processes that use them, if available • Check their digital signatures, if available • Check their base priorities, if available • Check the location they are being from, if available • Check their spellings, if available • Leverage memory analysis to detect hidden and/or injected process. Some malware can hide processes by unlinking them (among other ways). Memory analysis is a must these days, if available. • When you get comfortable with everything here, dig deeper and check what modules are typically loaded for each process, if available • Check and see if processes that should not be connecting out to the internet are not, if available • Check process privileges, if available • If wscript.exe process is running check the command line of what it is running, if available • Investigate processes running inside %temp%, root of %appdata%, %localappdata%, recycle bin, etc. , if available • If rundll32.exe is running check its command line as well, , if available • "Most" legitimate user applications like Adobe, Web browsers, etc. don't spawn child processes like cmd.exe. If you see this, they should be investigated. • Core Windows processes shouldn't be communicating out to the internet. If you see communication from these processes, dig deeper. Look for suspicious URLs/IPs, check process strings, etc. • Check and identify suspicious IP Addresses as well as sources identified as being outside BMO • Production trend the privileged activity and draft whitelists tactically and present to the ISOs and Compliance officers for review ad-hoc or within the CLM Splunk Log review forums accordingly. Log reviewers should also use the 13.15 dashboard – Event Code 4674 Analytics to help with the production trending and fine-tuning. Fine-tune the use case accordingly based on further investigations and consult Compliance officers and ISOs, where appropriate. Strategically, other correlation sources i.e. Carbon Black should be leveraged as integration sources and intelligence gathered to define whitelists accordingly.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation

	should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/30/2017 by Anthony DeMedeiros Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.15	
Use Case Title:	UCM 13.15 – Personal Privileged Activity – Unix/Linux UCM 13.15 – Generic Privileged Activity – Unix and Linux Analytics
Use Case Description:	Activity based report on personal privileged activity in Unix.
Context/Value:	Identify unauthorized privileged activity that may be occurring on Unix/Linux platforms.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Activity report to be trended to get to an exception based report
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** For any entries where 'In_AD' or 'In_ITIM' equals 0 indicates that the activity was performed by an ID not found in Active Directory or not within the user id book of record, ITIM. These cases should be followed up on immediately. Where In_AD and In_ITIM fields equal 1, these activities are performed by users that exist in Active Directory and ITIM. If the column "Dest_User_Privileged" has no data or is showing"0" then check Active Directory to identify if the ID is Privileged. If the ID is not Privileged then it should be considered an EOI. These cases should be scanned to ensure the user performing the activity reports into an authorized support manager. Any users who do not report into a manager or where the 'Destination_user_manager' is blank should also be investigated and validated against the Employee Directory. Furthermore, the appearance of an unknown privileged activity will need to be researched or verified with the Compliance officer and/or Information Security Officer (ISO) to determine appropriateness of the privileged activity. **Considerations:** **Checklist:** • Check the parent/child relationships of processes, if available • Check which users names the processes are running under, if available • Check their command line parameters for those processes that use them, if available • Check their digital signatures, if available • Check their base priorities, if available • Check the location they are being from, if available • Check their spellings, if available • Leverage memory analysis to detect hidden and/or injected process. Some malware can hide processes by unlinking them (among other ways). Memory analysis is a must these days, if available.

	• When you get comfortable with everything here, dig deeper and check what modules are typically loaded for each process, if available • Check and see if processes that should not be connecting out to the internet are not, if available • Check process privileges, if available • Check and identify suspicious IP Addresses as well as sources identified as being outside BMO • Production trend the privileged activity and draft whitelists tactically and present to the ISOs and Compliance officers for review ad-hoc or within the CLM Splunk Log review forums accordingly. Log reviewers should also use the UCM 13.15 – Generic Privileged Activity – Unix and Linux Analytics to help with the production trending and fine-tuning. Fine-tune the use case accordingly based on further investigations and consult Compliance officers and ISOs, where appropriate. Strategically, other correlation sources i.e. Carbon Black should be leveraged as integration sources and intelligence gathered to define whitelists accordingly.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/30/2017 by Anthony DeMedeiros
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.15	
Use Case Title:	UCM 13.15 – Generic Privileged Activity – iSeries
Use Case Description:	Exception based report on privileged activity on iSeries.
Context/Value:	Identify unauthorized privileged activity that may be occurring on iSeries.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** For any entries where 'In_AD' or 'In_ITIM' equals 0 indicates that the activity was performed by an ID not found in Active Directory or not within the user id book of record, ITIM. These cases should be followed up on immediately. Where In_AD and In_ITIM fields equal 1, these activities are performed by users that exist in Active Directory and ITIM. If the column "Dest_User_Privileged" has no data or is showing"0" then check Active Directory to identify if the ID is Privileged. If the ID is not Privileged then it should be considered an EOI. These cases should be scanned to ensure the user performing the activity reports into an authorized network support manager. Any users who do not report into a manager or where the 'Destination_user_manager' is blank should also be investigated and validated against the Employee Directory.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the

	procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 07/18/2017 by Anthony DeMedeiros
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 13.15 (Decommissioned – see 'Use Case Status' below for more details)	
Use Case Title:	UCM 13.15 – Generic Privileged Activity – Cisco
Use Case Description:	Exception based report on privileged activity on Cisco IOS/Nexus/ACS devices.
Context/Value:	Identify unauthorized privileged activity that may be occurring on Cisco devices such as IOS, Nexus and ACS.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See **'Anomalies'** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** Network configuration changes raised in this report during normal business hours are fairly rare and most changes should be taking place after business hours. Any changes made during business hours should be investigated and confirmed that an authorized CR was used. Any changes made with a shared/service ID should also be investigated immediately (Compliance officer should be involved). For any entries where 'In_AD' or 'In_ITIM' equals 0 indicates that the activity was performed by an ID not found in Active Directory or not within the user id book of record, ITIM. These cases should be followed up on immediately. Where In_AD and In_ITIM fields equal 1, these activities are performed by users that exist in Active Directory and ITIM. If the column "Dest_User_Privileged" has no data or is showing"0" then check Active Directory to identify if the ID is Privileged. If the ID is not Privileged then it should be considered an EOI. These cases should be scanned to ensure the user performing the activity reports into an authorized network support manager. Any users who do not report into a manager or where the 'Destination_user_manager' is blank should also be investigated and validated against the Employee Directory.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow	The original exception reports along with the evidence of the exception review (i.e. filters

up/resolution:	applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	• Approved on 04/24/2017 by Christine Dewhurst • Use Case DECOMMISSIONED on 09/15/2017 via CRUCM237 and approved by Elmer Valenzuela. The rationale is that Cisco privileged activity events have now been incorporated into UCM 13.15 – Network Generic Privileged Activity.
Next Review Date:	DECOMMISSIONED

UCM 13.15	
Use Case Title:	UCM 13.15 – Network Generic Privileged Activity
Use Case Description:	Exception based report on privileged activity on network devices (i.e. Cisco, NAB, Juniper, Alteon, Raritan incident, Bluecoat, Checkpoint, Nortel, BTINs, etc.).
Context/Value:	Identify unauthorized privileged activity that may be occurring on various network devices.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Access the LaaSException.Reporting@bmo.com mailbox on a daily basis and identify exceptions that require further follow up. Security Analyst submits Remedy ticket for any missing reports to the ISTS-Splunk team. For any content related issues, the Security Analyst will submit a Remedy ticket to the ISTS-Splunk team for resolution. 2. For any identified exceptions (See **‘Anomalies’** below). Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user’s manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. 3. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** For any entries where ‘In_AD’ or ‘In_ITIM’ equals 0 indicates that the activity was performed by an ID not found in Active Directory or not within the user id book of record, ITIM. These cases should be followed up on immediately. Where In_AD and In_ITIM fields equal 1, these activities are performed by users that exist in Active Directory and ITIM. If the column “Dest_User_Privileged” has no data or is showing”0” then check Active Directory to identify if the ID is Privileged. If the ID is not Privileged then it should be considered an EOI. These cases should be scanned to ensure the user performing the activity reports into an authorized network support manager. Any users who do not report into a manager or where the ‘Destination_user_manager’ is blank should also be investigated and validated against the Employee Directory.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.

Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 07/31/2017 by Anthony DeMedeiros – Network Devices
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 13.15	
Use Case Title:	UCM 13.15 – Windows Domain Policy changes
Use Case Description:	Exception based report on Windows Domain policy changes.
Context/Value:	Identify unauthorized configuration changes of systems. Will satisfy both SOX and PCI requirements.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception Alert
Recipient(s):	Security Analyst(s) (formerly Log Reviewer)
Actions performed:	1. Security analyst receives the UCM 12.1 *nix, Windows, and Cisco alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to follow up/investigate:** Any entries identified in the report mean that there was a deviation in the domain policy. The Security Analyst should follow up with the resource owner/COE support team to determine why there was a deviation from the Windows Domain Policy and was there an inheritance block put in place to perform this change (obtain and retain screen shot evidence of such changes). Any valid change to the Domain policy needs to be supported by an authorized change request.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow	Evidence of tracking, following up and resolution of any exceptions must be retained for

up/resolution:	at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/13/2017 by Anthony DeMedeiros
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.15b	
Use Case Title:	UCM 13.15b – Windows System Time Changes
Use Case Description:	Alert on any users making changes to server system time.
Context/Value:	Identify unauthorized changes to system time which can cause time stamps on event log entries to be inaccurate, time stamps on files and folders that are created or modified could be incorrect, computers that belong to a domain might not be able to authenticate themselves and users who try to log on to the domain from computers with inaccurate time might not be able to authenticate. Supports IS 10.01 Clock synchronization ISM requirement.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Alert
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives the UCM 13.15b System Time Change alert to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst creates a **Remedy ticket** and assigns it to the corresponding support team for follow up and investigation. The Security Analyst may engage CSOC IPC as necessary if they detect suspicious activity. A **logbook entry** is created for tracking of the alert. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/01/2017 by Christine Dewhurst
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 13.15e	
Use Case Title:	Kerberos Policy Changes
Use Case Description:	Any changes in Kerberos policy reported by current event must be monitored and an alert should be triggered. If this change was not planned, investigate the reason for the change. This evenet is generated only on domain controllers.
Context/Value:	Identify unauthorized changes to Kerberos policy on domain controllers. Kerberos policy is defined in GPOs linked to the root of the domain under Computer Configuration\Windows Settings\Security settings\Account Policy\Kerberos policy.
Owner:	Director of CyberSecurity Ops
Use Case Review Frequency:	At least annually.
Required output:	Alert
Recipient(s):	CSOC IPC
Actions performed:	Alert goes to CSOC IPC who triage, follow up and resolve as per the requirements of CSOC IPC playbook. CSOC IPC to communicate any compliance related feedback to the corresponding COE Compliance officers: 1. Elmer Valenzuela – EPS, CMRI 2. Allen Cui – NS 3. Nand Tonoo – DWS
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Alert goes to CSOC IPC via ArcSight ESM who triage, follow up and resolve as per the requirements of CSOC IPC playbook. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 04/27/2017 by Vicky Laurens
Next Review Date:	April 30, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 24.1	
Use Case Title:	Modification/Deletion of a Security Log – Linux Modification/Deletion of a Security Log – Unix Modification/Deletion of a Security Log – Windows & Cisco Modification/Deletion of a Security Log – iSeries Modification/Deletion of a Security Log – Network Devices
Use Case Description:	Exception Report (Alert) on any modification/deletion of security log files or when audit services are stopped on a compliance host for Windows flavours, Unix/Linux flavours, iSeries (leverages exception report only), Mainframe (leverages exception report only), and various types of Network Devices (Firewalls, routers, switches, etc.) prioritizing first critical, regulatory identified assets. (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity)
Context/Value:	Identify initialization of audit logs that could indicate that the log function was disabled by a user to hide their actions. Initialization, stopping, or pausing of the audit logs or turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	**Exception Report** (iSeries, Mainframe): Security Analysts (formerly Log Reviewers) **Exception Alert** (*nix, Windows, Cisco, Network Devices): Security Analysts (formerly Log Reviewers)
Recipient(s):	**Exception Report** (iSeries, Mainframe): Security Analysts (formerly Log Reviewers) **Exception Alert** (*nix, Windows, Cisco, Network Devices): Security Analysts (formerly Log Reviewers)
Actions performed:	**iSeries:** 1. Security analyst receives the UCM 24.1 Modification/Deletion of a Security Log - iSeries exception report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. Any non-IBM supplied ID that modifies/deletes the QAUDJRN should be immediately followed up on (Examples of IBM supplied profiles are QSYS, QPGRM (IBM supplied profiles/ID usually start with 'Q'). Non-IBM supplied profiles/ID that does not start with 'Q'modifying/deleting the audit journal should be followed up on. **Please Note:** while the QSECOFR account is considered an IBM supplied profile, as it is interactive, this account needs to be reviewed in all cases. To identify if the QSECOFR account is being used interactively, please correlate the events in this report with any events appearing in UCM 31.5 for iSeries. 2. Security analyst creates a **Remedy ticket** and assigns it to the corresponding support team for follow up and investigation. The Security Analyst may engage CSOC IPC as necessary if they detect suspicious activity. A **logbook entry** is created for tracking of the alert. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. ***nix, Windows, Cisco, & Network Devices:** 3. Security analyst receives the UCM 12.1 *nix, Windows, Cisco, and Network Device

	alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 4. Security analyst assesses the alert and identifies if there is an exception. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. Security Analysts to communicate any compliance related feedback to the corresponding COE Compliance officers: 1. Elmer Valenzuela – EPS, CMRI 2. Allen Cui – NS 3. Nand Tonoo – DWS
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	**iSeries, Mainframe:** Exception reports, logbook and any analysis performed on the reports should be retained for a period of at least 24 months (as per IMRR RRS – 1ADM25). ***nix, Windows, Cisco & Network Devices:** Exception Alert goes to Security Analyst via the LaaS Exception Reporting mailbox. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Use Case Status:	Approved on 12/07/2016 by Louise Dandonneau Approved on 07/10/2017 by Anthony DeMedeiros – iSeries
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 12/21/2017 by Anthony DeMedeiros

UCM 24.1	
Use Case Title:	Unauthorized access/modification/deletion of Mainframe security log
Use Case Description:	Exception report on any unauthorized access/modification/deletion of security log files (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity)
Context/Value:	Identify initialization of audit logs that could indicate that the log function was disabled by a user to hide their actions. Initialization, stopping, or pausing of the audit logs or turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Report
Recipient(s):	Security Analysts (formerly log reviewers)
Actions performed:	Mainframe: 1. Security analyst receives the UCM 24.1 to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst creates a **Remedy ticket** and assigns it to the corresponding support team for follow up and investigation. See '**Anomalies to be followed up on**' below. The Security Analyst may engage CSOC IPC as necessary if they detect suspicious activity. A **logbook entry** is created for tracking of the alert. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed up on:** Any mainframe, non-system, support group accessing the security logs should be followed up on with either the user's manager/account owner or RACF administrator. Refer to the 'Mainframe Support document v.1.3 for more details. Security analysts should develop a baseline/whitelist accordingly to assist in further fine-tuning the use case.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Security Analysts: Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25) (i.e. Remedy tickets, logbook, emails, etc.). Triaging, following up and resolution timeframes are based on ***LaaS Exception Handling Review Playbook: LaaS Exception Handling Review Response Times & Detail***.
Use Case Status:	Approved on 07/31/2017 by Anthony DeMedeiros – Mainframe zOS
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 24.1a	
Use Case Title:	Modification/Deletion of a Security Log – SYSTEM
Use Case Description:	Alert on any modification/deletion of security log files where 3 or more audit log clears within 24 hours through Windows SYSTEM account. Many audit log clears may indicate an underlying error condition or an event of interest.
Context/Value:	Identify initialization of audit logs that could indicate that the log function was disabled by a user to hide their actions. Initialization, stopping, or pausing of the audit logs or turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Alert
Recipient(s):	Security Analyst (formerly log reviewers)
Actions performed:	3. Security analyst receives the UCM 24.1a Modification/Deletion of a Security Log - SYSTEM alert to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 4. Security analyst creates a **Remedy ticket** and assigns it to the corresponding support team for follow up and investigation. The Security Analyst may engage CSOC IPC as necessary if they detect suspicious activity. A **logbook entry** is created for tracking of the alert. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25) (i.e. Remedy tickets, logbook, emails, etc.). Triaging, following up and resolution timeframes are based on ***LaaS Exception Handling Review Playbook: LaaS Exception Handling Review Response Times & Detail.*** .
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 12/06/2016 by Christine Dewhurst
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 12/21/2017 by Anthony DeMedeiros

UCM 24.2	
Use Case Title:	Access to security logs – Linux Access to security logs – Windows, Unix, Cisco Access to security logs – Mainframe zOS Access to security logs – iSeries Access to security logs – Checkpoint
Use Case Description:	Exception based report on users accessing or attempting to access security log files (based on the security log files of each flavour of Windows, mainframe, applications, iSeries, Unix, various network device types) per COE. The report should prioritize, but not limited to, critical, regulatory identified assets (This report should identify any user ID activity regardless of authority attempting to perform a specific privileged activity)
Context/Value:	Identify initialization of audit logs that could indicate that the log function was disabled by a user to hide their actions. Initialization, stopping, or pausing of the audit logs or turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually.
Required output:	Exception report that goes to a COE support manager/Security Analyst (formerly Log Reviewer) for action.
Recipient(s):	LaaS Exception Reporting mailbox monitored by a COE Support manager/Security Analyst (formerly log reviewer).
Actions performed:	1. COE support manager/Security analyst receives the UCM 24.2 exception report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com or COE support team's mailbox. 2. COE support manager/Security analyst opens the report and identifies any exceptions (see 'Anomalies to be followed up on' below) that need to be followed up on and creates a **Remedy ticket** and assigns it to the user's manager for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. 4. The COE support manager/Security Analyst can also leverage UCM 24.1 Modification/Deletion of Security logs to further triage and investigate any unauthorized changes. **Anomalies to be followed up on:** 1. An interactive user (privileged or non-privileged) attempting to 'read' the security log or any indication of attempting to 'modify' it should be followed up on. The Security Analyst should follow up with the user's manager if it is a non-privileged ID attempting to access the security log. 2. An interactive user (privileged or non-privileged) attempting to access the security log but "failed" to do so should be observed and further attention paid to subsequent attempts (success or failed) by the same user, and used as part of any evaluation related to Anomaly #1 above.
Use Case Sanity Validation: *(validating that use case is working as*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected.

expected in the production environment)	Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The exception reports are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the ***LaaS Exception Handling Review Playbook: LaaS Exception Handling Review Response Times & Detail.*** .
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 12/06/2016 by Christine Dewhurst Approved on 07/13/2017 by Anthony DeMedeiros – Mainframe OS Approved on 07/20/2017 by Anthony DeMedeiros – iSeries Approved on 07/31/2017 by Anthony DeMedeiros - Checkpoint
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 12/21/2017 by Anthony DeMedeiros

UCM 25 – Endpoints That Have Stopped Sending Logs to Splunk

UCM 25 results in Remedy tickets being created for endpoints that have stopped sending their logs to Splunk after a defined period of time. UCM 25 will identify any new log sourcetypes being ingested from an existing endpoint and incorporate that into monitoring. ISTS needs to ensure the index is onboarded properly to UCM 25 in order for the endpoints associated with that index to be monitored. Each endpoint has 'expected sourcetypes' associated with it and will be monitored by UCM 25. The expected sourcetypes can be found on the ISTS intranet site: Expected SourceType Reference.

The following features have been incorporated into UCM 25:

- **Remedy ticket generation throttling** – Remedy tickets generated will have a 'throttle' applied (max. 50) to avoid large numbers of Remedy tickets being created during a Splunk performance issue.
- **Anti-duplication** – avoids duplicate Remedy tickets being created for the same endpoint if a Remedy ticket already exists.
- **UCM 25 Exception lookup table** – for any endpoints that need to be exempt from UCM 25, the endpoints can be placed in this lookup table so that no Remedy tickets would be generated. This table can be used to manually exempt any servers that are in maintenance mode also.
- **Intelligent delays** - allows a healthy forwarder and low-risk sourcetypes to increase the time before a Remedy ticket is created. Some examples are 'linux:secure', 'aix:smit', etc. Since these sourcetypes don't typically have a lot of log events being ingested in a steady stream, they tend to generate a lot of 'false-positives' Remedy tickets. With the intelligent delay feature, we delay the creation of a Remedy ticket on low activity sourcetypes.
- **Active/Passive Clustering** - Logic has been added to check if a host is part of a cluster. If other cluster members are active and will not be created. All cluster members need to be added to the lookup for this mechanism to work and consider other cluster members. ISTS is able to add cluster members as required and upon request for applications and databases.
- **Automated Remedy ticket closure** – Splunk is able to detect when an endpoint that had once stopped logging, has started logging again. If the endpoint has started logging and there is an open Remedy ticket for it, Splunk will date/time stamp when the endpoint started logging again directly in the Remedy ticket and automatically close the ticket. This saves the endpoint support team time in manually closing the ticket and it also saves the TBCG Remediation team time in validating that the endpoint has started logging again and sending log events into Splunk.

UCM 25.2	
Use Case Title:	*Critical endpoints ('Idle' endpoints) that have stopped reporting and/or stopped sending required log events to Splunk. *Criticality defined by GITRM (Aman Raheja)
Use Case Description:	Alert on **critical**, open system (Windows, Unix/Linux), iSeries, and application/database endpoints that have stopped sending logs (idle endpoints) to Splunk production for greater than 12 hrs.
Context/Value:	Critical endpoints supporting the information security (GITRM) 'critical asset' definition, will be alerted on as not sending log events and the COE support teams will be sent Remedy tickets to act upon.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Alert translated into Remedy ticket
Recipient(s):	Remedy ticket: COE support team (support team identified via HPAM) Remedy queue Dashboard: COE production support managers/ISOs/Compliance officers/Executives Weekly 'Outstanding' Remedy report: Emailed report sent on a weekly basis to support teams
Actions performed:	**Alert triggers Remedy ticket automated creation:** 1. An alert is triggered when a *critical endpoint has stopped sending log events greater than 12 hours to Splunk Production for each 'expected sourcetype'**. ***Refer to the*** **'Splunk Endpoint Validation and Troubleshooting' for more *details on expected sourcetypes***. 2. The alert causes a Remedy ticket to be created and assigned to the appropriate COE support team's Remedy queue. The ticket is created based on the HPAM support group defined for the endpoint (responsibility lies on the endpoint owner to ensure HPAM data is kept current and up to date). 3. The COE support teams leverage their existing management process to resolve the Remedy ticket. SLAs are applied based on the Impact and Urgency. For **critical endpoints***, the SLA is defined as **'**Medium**'***** to get the endpoint logging again to Splunk. 4. The COE support teams can leverage the Endpoint Validation application and troubleshooting documentation on the GITRM LaaS Supporting Documents on the GITRM intranet site: https://intranet.bmogc.net/tando/gitrm/Pages/Services_Software/Other_Services/CLM/LaaS-Supporting-Documents.aspx 5. Where required, the COE support teams may need to work with application and database support teams for any application or database sourcetypes that are not sending log events from the required log source on the endpoint to Splunk. ***Criticality of endpoints is defined by GITRM.** **Depending on the sourcetype, different thresholds have been applied in order to ensure false-positive Remedy tickets are limited. ***the value was recommended to be 'Medium' priority by GITRM and now is being communicated to all COEs.
Additional reporting:	On a weekly basis, a UCM 25 Open/Outstanding Remedy ticket report is sent to all COE support teams to bring to their attention any unresolved tickets.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of

	reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Alerts and exception based reports must be retained for at least a period of 24 months (as per IMRR RRS – 1ADM25). All Remedy tickets generated as a result of alerts and/or exception based reports must also be retained for at least 24 months (as per IMRR RRS – 1ADM25) to demonstrate follow up and investigation of exceptions. Dashboards should also be retained for at least 24 months (as per IMRR RRS – 1ADM25) and evidence of action as a result of the dashboards should be tracked, logged and retained.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 04/24/2017 by Christine Dewhurst Approved on 06/29/2017 by Anthony DeMedeiros
Next Review Date:	April 30, 2019
Review Date Status:	Approved on 04/25/2018 by Anthony DeMedeiros

UCM 25.3 (formerly UCM 25.3a)	
Use Case Title:	*Non-critical endpoints (Idle endpoints) that have stopped reporting and/or stopped sending required log events to Splunk. *Criticality defined by GITRM (Aman Raheja)
Use Case Description:	An alert generated on non-critical endpoints, open system (Windows, Unix/Linux), application/database, and mainframe endpoints that have stopped sending log events from required log sources greater than 24 hrs.
Context/Value:	Non-critical endpoints supporting the information security (GITRM) 'critical asset' definition, will be alerted on as not sending log events and the COE support teams will be sent Remedy tickets to act upon.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Alert translated into Remedy ticket
Recipient(s):	Remedy ticket: COE support team (support team identified via HPAM) Remedy queue Dashboard: COE production support managers/ISOs/Compliance officers/Executives Weekly 'Outstanding' Remedy report: Emailed report sent on a weekly basis to support teams
Actions performed:	**Alert triggers Remedy ticket automated creation:** 1. An alert is triggered when a *non-critical endpoint has stopped sending log events greater than 24 hours to Splunk Production. 2. The alert causes a Remedy ticket to be created and assigned to the appropriate support team's Remedy queue. The Remedy queue the ticket is created for is based on the HPAM support group defined for the endpoint. 3. The COE support teams leverage their existing management process to resolve the Remedy ticket. SLAs are applied based on the Impact and Urgency. For **non-critical endpoints**, the SLA is defined as '**Low'*** to** get the endpoint logging again to Splunk. 4. The COE support teams can leverage the Endpoint Validation application and troubleshooting documentation on the GITRM LaaS Supporting Documents on the GITRM intranet site: https://intranet.bmogc.net/tando/gitrm/Pages/Services_Software/Other_Services/CLM/LaaS-Supporting-Documents.aspx. ***Refer to the '*****Splunk Endpoint Validation and Troubleshooting*****' for more *details on expected sourcetypes***. 5. Where required, the COE support teams may need to work with application and database support teams for any application or database sourcetypes that are not sending log events from the required log source on the endpoint to Splunk. ***Criticality of endpoints is defined by GITRM.** **Depending on the sourcetype, different thresholds have been applied in order to ensure false-positive Remedy tickets are limited. *** The value was recommended to be 'Low' priority by GITRM and now is being communicated to all COEs.
Additional reporting:	On a weekly basis, a UCM 25 Open/Outstanding Remedy ticket report is sent to all COE support teams to bring to their attention any unresolved tickets.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security

	analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Retention of triage/follow up/resolution:	Alerts and exception based reports must be retained for at least a period of 24 months (as per IMRR RRS – 1ADM25). All Remedy tickets generated as a result of alerts and/or exception based reports must also be retained for at least 24 months (as per IMRR RRS – 1ADM25) to demonstrate follow up and investigation of exceptions. Dashboards should also be retained for at least 24 months (as per IMRR RRS – 1ADM25) and evidence of action as a result of the dashboards should be tracked, logged and retained.
Use Case Status:	Approved on 04/24/2017 by Christine Dewhurst
Next Review Date:	April 30, 2019
Review Date Status:	Approved on 04/25/2018 by Anthony DeMedeiros

UCM 25.3e	
Use Case Title:	ESXi - *Non-critical endpoints (Idle endpoints) that have stopped reporting and/or stopped sending required log events to Splunk *Criticality defined by GITRM (Aman Raheja)
Use Case Description:	An alert generated on non-critical endpoints, open system ESXi endpoints that have stopped sending log events from required log sources greater than 24 hrs.
Context/Value:	Non-critical endpoints supporting the information security (GITRM) 'critical asset' definition, will be alerted on as not sending log events and the COE support teams will be sent Remedy tickets to act upon. Specific to ESXi devices, as long as the VMWare host is still sending at least one ESXi sourcetype it will not trigger a UCM 25 alert. If no ESXi sourcetypes report within 24 hours, a Remedy incident will be generated for that host.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Alert translated into Remedy ticket
Recipient(s):	Remedy ticket: COE support team (support team identified via HPAM) Remedy queue Dashboard: COE production support managers/ISOs/Compliance officers/Executives Weekly 'Outstanding' Remedy report: Emailed report sent on a weekly basis to support teams
Actions performed:	**Alert triggers Remedy ticket automated creation:** 1. An alert is triggered when a *non-critical endpoint has stopped sending log events greater than 24 hours to Splunk Production. 2. The alert causes a Remedy ticket to be created and assigned to the appropriate support team's Remedy queue. The Remedy queue the ticket is created for is based on the HPAM support group defined for the endpoint. 3. The COE support teams leverage their existing management process to resolve the Remedy ticket. SLAs are applied based on the Impact and Urgency. For **non-critical endpoints**, the SLA is defined as '**Low'*** to** get the endpoint logging again to Splunk. 4. The COE support teams can leverage the Endpoint Validation application and troubleshooting documentation on the GITRM LaaS Supporting Documents on the GITRM intranet site: https://intranet.bmogc.net/tando/gitrm/Pages/Services_Software/Other_Services/CLM/LaaS-Supporting-Documents.aspx. ***Refer to the* '*Splunk Endpoint Validation and Troubleshooting*' for more *details on expected sourcetypes***. 5. Where required, the COE support teams may need to work with application and database support teams for any application or database sourcetypes that are not sending log events from the required log source on the endpoint to Splunk. ***Criticality of endpoints is defined by GITRM.** **Depending on the sourcetype, different thresholds have been applied in order to ensure false-positive Remedy tickets are limited. *** The value was recommended to be 'Low' priority by GITRM and now is being communicated to all COEs.
Additional reporting:	On a weekly basis, a UCM 25 Open/Outstanding Remedy ticket report is sent to all COE support teams to bring to their attention any unresolved tickets.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to

	consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Retention of triage/follow up/resolution:	Alerts and exception based reports must be retained for at least a period of 24 months (as per IMRR RRS – 1ADM25). All Remedy tickets generated as a result of alerts and/or exception based reports must also be retained for at least 24 months (as per IMRR RRS – 1ADM25) to demonstrate follow up and investigation of exceptions. Dashboards should also be retained for at least 24 months (as per IMRR RRS – 1ADM25) and evidence of action as a result of the dashboards should be tracked, logged and retained.
Use Case Status:	Approved on 05/03/2018 by Anthony DeMedeiros
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 05/03/2018 by Anthony DeMedeiros

UCM 25.4	
Use Case Title:	Network device endpoints (Idle endpoints) that have stopped reporting and/or stopped sending required log events to Splunk after a defined period of time.
Use Case Description:	An alert generated on network device endpoints i.e. Cisco, Juniper, Checkpoint, etc., that have stopped sending log events from required log sources greater than ***7 days**.
Context/Value:	Network device endpoints will be alerted on as not sending log events to Splunk and the COE support teams will be sent Remedy tickets to act upon them to ensure they don't become idle. Network device activity differs from network device type to network device type. ***Rationale for 7 day threshold:** 1. At the time of Splunk onboarding, endpoints have a standard logging configuration applied **AND** are validated in Splunk as logs being ingested. 2. A heartbeat already exists for operational purposes (all network devices are polled via SNMP every 5 or 15 minutes) – so if there is a problem with a device the NOC will be aware. 3. All network support teams monitor for deviations in logging configurations. Unless the logging configuration is changed, the network devices should continue to send logs accordingly to Splunk. 4. All support teams have access to the Splunk Endpoint validation application to validate the status of logging of their endpoints at any given time. 5. UCM 13.1 – Logging configuration changes alerts the appropriate stakeholders (i.e. security analysts/CSOC IPC) of changes to audit logging configuration changes. 6. Backups of configurations are performed on network devices at least once a week so backup log events are sent to Splunk at least weekly indicating logs are being sent to Splunk on a defined basis (it's difficult to gauge when members of clusters go from 'active' to 'passive' or are legitimately idle for a prolonged period of time). Taking all of the above into consideration, UCM 25.2 and UCM 25.3, the appropriate threshold is greater than 7 days to validate that a network device endpoint has stopped sending logs. Other considerations: • The support teams have stated that due to active/passive members of cluster pairs of some network endpoints, some members could legitimately be idle for prolonged periods of time – this is normal and expected behavior. • There's no easy way to establish Splunk logic to identify 'true' NS idle endpoints and we would be creating a lot of 'false-positive' Remedy tickets for NS support teams to investigate.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Alert translated into Remedy ticket
Recipient(s):	Remedy ticket: COE support team (support team identified via HPAM) Remedy queue Dashboard: COE production support managers/ISOs/Compliance officers/Executives Weekly 'Outstanding' Remedy report: Emailed report sent on a weekly basis to support teams
Actions performed:	**Alert triggers Remedy ticket automated creation:** 1. An alert is triggered when a network device endpoint has stopped sending log events greater than 7 days to Splunk Production. 2. The alert causes a Remedy ticket to be created and assigned to the appropriate support team's Remedy queue. The Remedy queue the ticket is created for is based on the

	HPAM support group defined for the endpoint. 6. The COE support teams leverage their existing management process to resolve the Remedy ticket. SLAs are applied based on the Impact and Urgency. For **non-critical endpoints**, the SLA is defined as **'Low'** to get the endpoint logging again to Splunk. For critical endpoints, the SLA is defined as '**Medium**' to get the endpoint logging again to Splunk 7. The COE support teams can leverage the Endpoint Validation application and troubleshooting documentation on the GITRM LaaS Supporting Documents on the GITRM intranet site: https://intranet.bmogc.net/tando/gitrm/Pages/Services_Software/Other_Services/CLM/LaaS-Supporting-Documents.aspx
Additional reporting:	On a weekly basis, a UCM 25 Open/Outstanding Remedy ticket report is sent to all COE support teams to bring to their attention any unresolved tickets.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Retention of triage/follow up/resolution:	Alerts and exception based reports must be retained for at least a period of 24 months (as per IMRR RRS – 1ADM25). All Remedy tickets generated as a result of alerts and/or exception based reports must also be retained for at least 24 months (as per IMRR RRS – 1ADM25) to demonstrate follow up and investigation of exceptions. Dashboards should also be retained for at least 24 months (as per IMRR RRS – 1ADM25) and evidence of action as a result of the dashboards should be tracked, logged and retained.
Use Case Status:	Approved on 04/24/2017 by Christine Dewhurst
Next Review Date:	April 30, 2019
Review Date Status:	Approved on 04/25/2018 by Anthony DeMedeiros

UCM 30.1	
Use Case Title:	Authentication failure (failed login attempts) for remote access (i.e. VPN)
Use Case Description:	Alert on failed login attempts greater than 10 attempts in less than one minute per user.
Context/Value:	Identify unauthorized access.
Owner:	Director of CyberSecurity Ops
Use Case Review Frequency:	At least annually
Required output:	Alert
Recipient(s):	CSOC IPC triage the alerts
Actions performed:	Alert goes to CSOC IPC who triage, follow up and resolve as per the requirements of CSOC IPC playbook based on specific security events of interest. CSOC IPC to communicate any compliance related feedback to the corresponding COE Compliance officers: 1. Elmer Valenzuela – EPS, CMRI 2. Allen Cui – NS 3. Nand Tonoo - DWS
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Alert goes to CSOC IPC via IPC@bmo.com account that triage, follow up and resolve as per the requirements of CSOC IPC playbook. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Use Case Status:	Approved on 11/03/2016 by Louise Dandonneau
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 01/02/2018 by Vicky Laurens

UCM 30.1a	
Use Case Title:	Authentication failure (failed login attempts) for remote access (i.e. VPN)
Use Case Description:	Alert on failed login attempts greater than 10 attempts in less than one minute by multiple users per source IP
Context/Value:	Identify unauthorized access.
Owner:	Director of CyberSecurity Ops
Use Case Review Frequency:	At least annually
Required output:	Alert
Recipient(s):	CSOC IPC triage the alerts
Actions performed:	Alert goes to CSOC IPC who triage, follow up and resolve as per the requirements of CSOC IPC playbook based on specific security events of interest. CSOC IPC to communicate any compliance related feedback to the corresponding COE Compliance officers: 1. Elmer Valenzuela – EPS, CMRI 2. Allen Cui – NS 3. Nand Tonoo - DWS
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Alert goes to CSOC IPC via IPC@bmo.com account that triage, follow up and resolve as per the requirements of CSOC IPC playbook. Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Use Case Status:	Approved on 11/03/2016 by Louise Dandonneau
Next Review Date:	December 31, 2018
Review Date Status:	Approved on 01/02/2018 by Vicky Laurens

UCM 31.1 (Decommissioned – see 'Use Case Status' below for more details)	
Use Case Title:	Deletion of user/group account in applications.
Use Case Description:	Exception report on deletion of user/group accounts within applications
Context/Value:	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception report
Recipient(s):	Security Analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives the UCM 31.1 exception report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst opens the report and identifies any exceptions (see '**Anomalies to be followed up on' below**) that need to be followed up on and creates a **Remedy ticket** and assigns it to the user's manager/ID owner for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on:** Security analysts should follow up on any user that removes/deletes user/group accounts where In_AD=0 or In_ITIM=0 immediately as it may indicate a malicious unauthorized account that may have been in use and being deleted/removed to hide its actions. Security analysts should also develop whitelists and baselines to assist in identifying further anomalies and help to further fine-tune the use case. Information security officers/CSOC IPC should be engaged, where appropriate, by the Security analysts.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Use Case Status:	Use Case DECOMMISSIONED on 07/18/2017 as per request from David Lachmansingh. The rationale is UCM 31.1's events will now fall under UCM 31.3 which will cover off user and group creations/modifications/deletions.
Next Review Date:	DECOMMISSIONED

UCM 31.2	
Use Case Title:	Elevation of access on Bluecoat devices. Elevation of access within applications (i.e. Users being placed into groups with more access or being given access privileges higher than what they had before) Elevation of access within databases Elevation of access – Network Devices (Checkpoint, Cisco, Juniper, Nortel, Fireeye) Elevation of access – VBOS Elevation of access - Middleware
Use Case Description:	Exception Report on elevation of access on Bluecoat devices, various applications, VBOS, and Middleware Exception Alert on elevation of access on Databases (Oracle, SQL)
Context/Value:	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Report Exception Alert – Oracle, SQL
Recipient(s):	Security Analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives the UCM 31 exception report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst opens the report and identifies any exceptions (see 'Anomalies to be followed up on' below) that need to be followed up on and creates a **Remedy ticket** and assigns it to the user's manager/ID owner for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Security Analyst – Exception Alert (Oracle, SQL):** 1. Security analyst receives the UCM 31.2 Oracle or SQL alert to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other

	supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Anomalies to be followed up on:** **Bluecoat:** Security analysts should follow up on any user that receives 'administrative' privileges to Bluecoat devices to ensure access is authorized. Security analysts should also develop whitelists and baselines to assist in identifying further anomalies and help to further fine-tune the use case. Information security officers/CSOC IPC should be engaged, where appropriate, by the Security analysts. **Applications/Databases/Network devices:** Security analysts should follow up on any user that appears in the report to ensure access is authorized. Particular focus and follow up should be on those users where In_AD=0 or In_ITIM=0. Security analysts should also develop whitelists and baselines to assist in identifying further anomalies and help to further fine-tune the use case. Application support teams, Information security officers/CSOC IPC should be engaged, where appropriate, by the Security analysts for further guidance.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Use Case Status:	Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/20/2017 by Anthony DeMedeiros - Applications Approved on 07/21/2017 by Anthony DeMedeiros – Databases (Oracle) Approved on 07/28/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 07/31/2017 by Anthony DeMedeiros - Databases (Sybase) Approved on 07/27/2017 by Anthony DeMedeiros - Network devices (Checkpoint) DECOMMISSIONED on 12/07/2017 via CRUCM468 and approved by Anthony DeMedeiros for Network Devices. The rationale is that any access to a network device is considered privileged. UCM 13.15 already captures all privileged activity for network devices. UCM 13.8/UCM 13.12 captures specific changes to configurations to network devices also. Accessing a network device is only possible through an existing privileged or root/administrator account and changes to these accounts (if any) would fall under the scope of UCM 31.3. For these reasons above, UCM 31.2 for Network Devices is no longer required.

Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 31.2a	
Use Case Title:	Alert on elevation of access into a built-in Windows privileged group (i.e. Enterprise Administrators, Schema Administrators, Administrators, Domain Administrators, Server Operators, Account Operators and Backup Operators)
Use Case Description:	Alert on any user/ID added to any of the following groups: ● Enterprise Administrators ● Schema Administrators ● Administrators ● Domain Administrators ● Server Operators, ● Account Operators ● Backup Operators
Context/Value:	Without knowing who was logged on at the time of an event, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director of CyberSecurity Ops
Use Case Review Frequency:	At least annually
Required output:	Alert
Recipient(s):	CSOC IPC triage the alerts
Actions performed:	Alert goes to CSOC IPC who triage, follow up and resolve as per the requirements of CSOC IPC playbook based on specific security events of interest. CSOC IPC to communicate any compliance related feedback to the corresponding COE Compliance officers: 1. Elmer Valenzuela – EPS, CMRI 2. Allen Cui – NS 3. Nand Tonoo – DWS
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on CSOC IPC playbooks.
Use Case Status:	Approval on 01/18/2017 by Vicky Laurens
Next Review Date:	January 31, 2019
Review Date Status:	Approved on 04/06/2018 by Vicky Laurens

UCM 31.2c	
Use Case Title:	Elevation of access using 'su' and 'sudo' successfully – Unix and Linux
Use Case Description:	Exception based report on those accounts/user IDs that successfully 'su'/'sudo' into a privileged ID such as root.
Context/Value:	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Reports (below): • UCM 31.2c (*nix) - Elevation of access using 'su' and 'sudo' successfully – Source User **is not** "root" • UCM 31.2r (*nix) - Elevation of access using 'su' and 'sudo' successfully – Source & Destination Users **are** "root"
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives the UCM 31.2c & UCM 31.2r ('su' and 'sudo' successful) exception reports to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst opens the report and identifies any exceptions (see 'Anomalies to be followed up on' below) that need to be followed up on and creates a **Remedy ticket** and assigns it to the user's manager/ID owner for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Log Reviewer Focus:** i. Log Reviewers are to prioritize their review based on the high risk scenario of all "su" or "sudo" commands where the source user **is not** "root" (UCM 31.2c). This report contains only those events where a unique ID is found to have 'su' or 'sudo'-ed to 'root' or any other generic privileged ID. This will assist with prioritizing events which might be indicative of unauthorized or abnormal activities (such as a non-adm account executing this) ii. Log Reviewers are to also review the UCM 31.2r report as this provides a comprehensive view of "su" or "sudo" commands where the source and destination users **are** "root". This report contains only those events where both the source and destination user are 'root'. This will help with identifying instances where accountability cannot be established for the use of 'root' on a particular device **Anomalies to be followed up on:** Successful 'switch user' (su) or 'sudo' into a privileged ID by a user/ID other than an administrator or not within AD.
Use Case Sanity Validation:	On at least a semi-annual basis or as required, the use case owner is responsible for

(validating that use case is working as expected in the production environment)	testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 02/28/2017 by Christine Dewhurst
Next Review Date:	January 31, 2019
Review Date Status:	Approved on 02/08/2018 by Anthony DeMedeiros

UCM 31.3	
Use Case Title:	User Account and Group Changes for Windows, applications, network devices i.e. Bluecoat, databases, iSeries, Tandem, VBOS, VMWare, Middleware, and Mainframe
Use Case Description:	A report on User and Group Account Changes for Windows, applications, network devices, databases, iSeries, Tandem, VBOS, VMWare, Middleware, and Mainframe
Context/Value:	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	Security analyst receives the UCM 31.3 'unfiltered' (Windows) report, UCM 31.3 (Applications), UCM 31.3 (Mainframe Applications), UCM 31.3 (Mainframe Databases), UCM 31.3 (Databases), UCM 31.3 (iSeries), UCM 31.3 (Tandem), UCM 31.3 (Mainframe) and UCM 31.3 (Bluecoat) to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. **Windows:** 1. Security analyst opens the report and filters the report based on 'Source User Manager' (see 'Overview') and leverages the list of 'authorized' support teams able to make user and group changes. Any exceptions identified need to be followed up on with the user manager by creating a **Remedy ticket** and **email** assigning it to the COE Remedy support queue. The Security analyst should send an email to the 'Source User Manager' to advise of the ticket created and that they are required to review the activity of their immediate user/employees who have performed the actions and identify any non-compliance activities and correct it immediately. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. For any non-compliance issues identified by the 'Source User Manager' of activities that were performed by their employee's, the Security analyst must request that the Source User Manager correct the non-compliance issue before closing the Remedy ticket. 2. A **logbook entry** is created for tracking of any identified exceptions. If the report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. 3. The Security Analyst provides feedback to the ISTS team on fine-tuning opportunities identified as a result of feedback from the 'Source User Managers' in #2 above. COE compliance officers as well as COE ISO's should be consulted and approve the fine-tuning opportunities to ISTS. This should be performed daily until a 'filtered' version of 31.3 can be created (once all user IDs are onboarded to CyberArk, this use case will likely be decommissioned) to make it more exception-based reporting.

Overview:

At the time of establishing this use case, accountabilities/responsibility for access management/user provisioning was distributed to several support groups across the bank including. The managers of these groups can be found below and a list of 'authorized' support team members and managers able to make such changes:

GITRM IAM:

- Amanda Wilcox, Ahmar Nadeem, Dawn Boonstra – amending global and universal security groups

AD Operations:

- Affan Syed – amending GPO objects as a part of the asset disposal process.
- Karen Willis – amending local security groups associated to workstations.
- Anthony Lo – amending deleting groups related to Outlook objects.

CMRI's Global Access Management group:

- Katherine Grishaber – amending IBG global and security groups
- James Price - amending local security groups associated to workstations.
- Mihaly Balint - amending all types of groups.

Other Source User Managers:

- Orele Pluck, Jeffrey Bronski, James Price, Helen Mintsopoulos, Adrian Smith

Technology Help Desk Managers:

- Giurleo,Nick
- Daley, Fiona
- Dallaire, Vic
- Inglis, Reba

Technology Field Services Support:

- Klich,Christine
- Wong, Serena
- Persaud, Andrew

Log reviewers should immediately follow up on any 'non-adm' users making any user provisioning changes with the user's manager and engage the Compliance officer/ISO as required.

Applications/Databases:

Security Analysts need to trend the production reports and follow up on creations/modifications/deletions to ensure they were appropriately authorized before they were created/modified/deleted. The Security Analyst must also continue to fine-tune the report and obtain lists of all authorized application support personnel able to provision user/groups accounts by contacting each application support group.

Network Devices:

Security Analysts need to trend the production reports and follow up on creations/modifications/deletions to ensure they were appropriately authorized before they were created/modified/deleted and follow up on any user/accounts used to make the changes where In_AD=0 or In_ITIM=0. The Security Analyst must also continue to fine-tune the report and obtain lists of all authorized network support personnel able to provision user/groups accounts by contacting the support

	team that supports these network devices. **iSeries:** Security Analysts need to trend the production reports and follow up on creations/modifications/deletions to ensure they were appropriately authorized before they were created/modified/deleted. The Security Analyst must also continue to fine-tune the report and obtain lists of all authorized support personnel able to provision user/groups accounts by contacting the support team that supports the iSeries. **Tandem:** Security Analysts need to trend the production reports and follow up on creations/modifications/deletions to ensure they were appropriately authorized before they were created/modified/deleted. The Security Analyst must also continue to fine-tune the report and obtain lists of all authorized support personnel able to provision user/groups accounts by contacting the support team that supports the Tandem. **Mainframe:** Security Analysts need to trend the production reports and follow up on creations/modifications/deletions to ensure they were appropriately authorized before they were created/modified/deleted. The Security Analyst must also continue to fine-tune the report and obtain lists of all authorized support personnel able to provision user/groups accounts by contacting the support team that supports the Mainframe. **Mainframe Applications/Databases:** Security Analysts need to trend the production reports and follow up on creations/modifications/deletions to ensure they were appropriately authorized before they were created/modified/deleted. The Security Analyst must also continue to fine-tune the report and obtain lists of all authorized support personnel able to provision user/groups accounts by contacting the support team that supports the Mainframe applications/databases. Identity Access Management (Christy Flood) should be engaged regularly to get an updated list of authorized managers from Aveksa who support user provisioning.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 03/13/2017 by Christine Dewhurst - Servers Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/21/2017 by Anthony DeMedeiros – Databases (Oracle) Approved on 07/28/2017 by Anthony DeMedeiros – Databases (MS SQL)

	Approved on 07/31/2017 by Anthony DeMedeiros - Databases (Sybase) Approved on 07/21/2017 by Anthony DeMedeiros - iSeries Approved on 07/31/2017 by Anthony DeMedeiros - Mainframe Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe Applications Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe Databases Approved on 01/29/2018 by Anthony DeMedeiros – Tandem
Next Review Date:	March 31, 2019
Review Date Status:	Approved on 03/29/2018 by Anthony DeMedeiros

UCM 31.3a	
Use Case Title:	User Account and Group Changes for Privileged built-in groups - Windows
Use Case Description:	A report/alert on User and Group Account Changes for Privileged built-in groups - Windows
Context/Value:	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Report - iSeries, Oracle, PostgreSQL, SQL, Sybase, Network, and Application Exception Alert – Windows/*nix
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	• Security analyst receives UCM 12.1 iSeries, Oracle, PostgreSQL, SQL, Sybase, Network, and Application alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. • Security analyst assesses the alert and identifies if there is an exception. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. **Windows/*nix:** 1. Security analyst receives the UCM 31.3a Windows/*nix alert to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception (see '**Anomalies to be followed up on**' below) that needs to be followed up on and creates a **Remedy ticket** and assigns it to the appropriate user support group for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate

	directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on:** Any user who makes a change outside of the DWS AD Operations is an exception.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 02/28/2017 by Christine Dewhurst
Next Review Date:	February 28, 2019
Review Date Status:	Approved on 03/01/2018 by Anthony DeMedeiros

UCM 31.3d	
Use Case Title:	User Account and Group Changes for Unix/Linux platforms
Use Case Description:	A report on User and Group Account Changes for Unix/Linux platforms that contains 'root' user provisioning/access management activities (only 'root' account is permitted to perform user provisioning activities/access management activities). A dashboard (UCM 31.2c dashboard) to be leveraged that indicates 'su' and 'sudo' level activities performed by unique users to correlate the report to (unique user -> su or sudo -> root).
Context/Value:	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives the UCM 31.3d report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. The Security Analyst also has access to the UCM 31.2c dashboard to correlate su and sudos to root activity. If the Security Analyst can correlate su and sudos (via data/time) to authorized users who have performed these actions/activities on the endpoint, then no further action is required. 2. Security analyst opens the report and identifies any exceptions (see 'Anomalies to be followed up on' below) that need to be followed up on and creates a **Remedy ticket** and assigns it to the user's manager/ID owner for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on:** For any user provisioning/access management change in the report that **cannot** be correlated back to the 31.2c dashboard, it is an indication that someone has potentially logged directly into 'root' to perform user provisioning activities **without** su/sudo'ing in. BMO's policy is that no one directly logs into root (except from the system console). NOTE: CMRI uses a tool called Puppet to push batch user provisioning changes to endpoints. Puppet assumes 'root' to provision user accounts.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use

	cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 04/03/2017 by Christine Dewhurst
Next Review Date:	April 30, 2019
Review Date Status:	Approved on 04/25/2018 by Anthony DeMedeiros

UCM 31.3e	
Use Case Title:	User Account and Group Changes for Cisco ACS
Use Case Description:	A report on User and Group Account Changes for Cisco IOS platforms. This will report on all activity performed at the Cisco ACS device level which allows users and groups to be added/modified/deleted.
Context/Value:	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives the UCM 31.3e report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst opens the report and identifies any exceptions (see 'Anomalies to be followed up on' below) that need to be followed up on and creates a **Remedy ticket** and assigns it to the appropriate support group for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on:** For any users who created/modified/deleted the destination user/group (i.e. the user/group who was created/modified/deleted) and who do not appear in AD (In_AD=0) or in ITIM (In_ITIM=0) should be followed up on. Any users who add/modify/delete a user/group who doesn't report into a Network Service production support/engineering/service delivery manager should also be investigated and followed up on.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 04/03/2017 by Christine Dewhurst

Next Review Date:	April 30, 2019
Review Date Status:	Approved on 04/25/2018 by Anthony DeMedeiros

UCM 31.4	
Use Case Title:	Successful login by Terminated Employees
Use Case Description:	An exception based report which reports on access by any terminated employee, expired contractor, or other expired account on Windows, applications, databases, Linux and Unix flavours and Network device types.
Context/Value:	Identify unauthorized access. To identify a security breach/operational issue due to the activity is occurring often/high volume event. If an employee has left the company and still has access to the network via their user account, unnecessary or malicious access to sensitive/confidential data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account. To prevent unauthorized access, user credentials and other authentication methods therefore need to be revoked promptly (as soon as possible) upon the employee's departure.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Report
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives the UCM 31.4 report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst opens the report and identifies any exceptions (see 'Anomalies to be followed up on' below) that need to be followed up on and creates a **Remedy ticket** and assigns it to the appropriate support group for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on (Windows):** • For any users with 'Weekdays_Since_Termination' > 10 and a termination date identified, use the following checklist and consult a Compliance officer and other enrichment sources i.e. EDS query, where required based on the following: An ID from a terminated employee has been accessed (login) beyond 10 business days, thus presenting a contradiction of ISM requirements specific to the suspension and deletion of ID`s. The above condition adheres to two requirements of the ISM, specifically: **ISM 05.02.1 – 2a – Suspension and Deletion of ID's:** ID Owners (e.g., Unit Managers) shall promptly change/suspend the access authorities for an individual, in the event of a staffing change (e.g., termination, resignation, change in assignment/department), following the appropriate change management process.

ISM 05.02.1 – 2f – Suspension and Deletion of ID's:
An individual ID that has been suspended or disabled, and the original user has left the employ of the Enterprise, the re-assignment or re-enablement of the ID to the user's previous management shall be permitted:

- For data recovery purposes
- For a limited period of time, not exceeding 10 business days

For instances that exceed the ISM requirement the following condition scenarios may be present and should be considered before escalation procedures are invoked:

1

Condition Scenario:
The ID may have been reassigned as a functional ID by the manager or department. This would likely be associated with older ID's (legacy).

Action to be taken:
The likelihood of this occurrence can be identified through the Event Count associated with a given ID. Log Reviewers should consider the volume of count as part of their investigation – a high volume likely signifies that the ID is being used in a functional manner rather than a personal manner, provided that the ID name appears to be a Personal ID rather than a Service/Functional ID. The Log Reviewer should request from management if an ISM exception is present for the ID and record this information for future reference. If there is no exception in place they are then to be directed to seek an exception and they are to engage their Information Security Officer immediately. Management is also requested to contact Identify Access Management (GITRM) to ensure appropriate set up of the ID in question as to ensure that it remains in keeping with ISM requirements specific to Access Management. A continued repeat of the event of interest for the specific ID should be escalated with management and Identity Access Management representatives as an alert on the inappropriate use of a personal ID for functional purposes.

Additional Support Information: Logon Type has been added to the report which provides further insight regarding the actual usage of the ID which can further assist Log Reviewers in determining the status of the ID and its purpose.

Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unattended workstation with password protected screen saver)
8	Network Cleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication")
9	New Credentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials, reference Event ID 4648
10	Remote Interactive (Terminal Services, Remote Desktop or Remote Assistance)
11	Cached Interactive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

	2	**Condition Scenario:** The employee may be contracted staff. There may be some instances where a contractor may be terminated and rehired within a short period of time. As per HR policy managers are required to commence with access removal requests in advance of final date of the contracted employee. De-provisioning may be underway or completed at the time that the manager requests provisioning of the same ID(s). **Action to be taken:** The likelihood of this occurrence is limited and should be followed up with management for confirmation that proper Access Management MACD processes have been followed. If the manager has followed the proper process the alert for the specific ID should not be produced again. A continued repeat of the event of interest for the specific ID should be escalated with management.
	3	**Condition Scenario:** The employee may have been notified of advanced termination resultant of planned staff reduction. At manager's discretion and following HR policy, they are required to commence with access removal requests in advance of the final date of the employee. The employee may be designated as terminated through HR process, but they remain functionally active until their termination date. **Action to be taken:** The likelihood of this occurrence is reasonable and should be followed up with management for confirmation of the condition. Upon termination date and if the manager has followed the proper Access Management MACD process, the alert for the specific ID should not be produced again. A continued repeat of the event of interest for the specific ID should be escalated with management.
	4	**Condition Scenario:** The employee may be on Short Term or Long Term Leave. At manager's discretion and following HR policy, they are required to commence with access suspension requests. The employee may be designated as inactive or STD/LTD through HR process, but they may remain functionally active through an arrangement with their manager. **Action to be taken:** The likelihood of this occurrence is limited and should be followed up with management for confirmation of the condition. This condition may not result in a satisfactory outcome until the employee returns to work and their HR status is returned back to Active. *Further investigation of this condition may be required in order to determine Employee Status types that can be used to further filter down this condition.*
	5	**Condition Scenario:** Management may not have fully followed the Access Management MACD process for a terminated employee. An example would be that a request for access removal may not have included all ID's for an employee, which may result in notification that the employee status is terminated but their AD ID remains active. **Action to be taken:**

	The likelihood of this occurrence is reasonable and should be followed up with management for confirmation of the condition. If the manager has followed the proper process the alert for the specific ID should not be produced again. A continued repeat of the event of interest for the specific ID should be escalated with management.
6	**Condition Scenario:** The ID in question may have been recycled (to be confirmed). Although the ID appears as terminated, the owner of the ID may have changed over time (same full name or different first name that begins with the same initial, e.g. Old ID is Steve Jones = SJONES, New ID is Stan Jones = SJONES). **Action to be taken:** The likelihood of this occurrence presents a challenge and should be followed up with management for confirmation of the condition. Synchronization of the various Access Management databases is likely required to ensure that old information related to the ID is updated to reflect currency. *Further investigation of this condition may be required in order to determine how to deal with this type of condition.*

- Where the 'Weekdays_Since_Termination' is blank and the Termination Date is blank, the above table should be considered also. Compliance officers should be engaged/consulted accordingly for further analysis/follow-up, where required and corrective action undertaken.

Anomalies to be followed up on (databases):

- Security analysts should leverage the OS version of 31.4 to ensure that the AD access has been terminated accordingly. If the AD access has been terminated/disabled ('front door' access), then the database access should be 'housekeeping' and the database access management team should remove the access accordingly. Compliance officers should be engaged/consulted accordingly for further analysis/follow-up, where required and corrective action undertaken.

Anomalies to be followed up on (applications):

- Security analysts should leverage the OS version of 31.4 to ensure that the AD access has been terminated accordingly. If the AD access has been terminated/disabled ('front door' access), then the application access should be 'housekeeping' and the application access management team should remove the access accordingly. Compliance officers should be engaged/consulted accordingly for further analysis/follow-up, where required and corrective action undertaken.

Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).

Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 05/30/2017 by Anthony DeMedeiros Approved on 07/19/2017 by Anthony DeMedeiros – Databases Approved on 07/28/2017 by Anthony DeMedeiros – Databases (MS SQL) Approved on 07/20/2017 by Anthony DeMedeiros - Applications Approved on 07/28/2017 by Anthony DeMedeiros – Network Devices
Next Review Date:	May 31, 2019
Review Date Status:	Approved on 06/13/2018 by Anthony DeMedeiros

UCM 31.5	
Use Case Title:	Access by Privileged accounts Successful login to QSECOFR Successful login to SUPER.SUPER
Use Case Description:	**Application/Database**: An exception based report on access of privileged accounts for databases, and various applications. **iSeries**: An exception based alert on successful logins to QSECOFR **Tandem:** An exception based alert on successful logins to SUPER.SUPER (255,255) **VMWare:** An exception based report on access of privileged accounts for VMWare
Context/Value:	Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Report – Application/Database, Tandem, VMWare Exception Alert – iSeries
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	**Applications/Databases/Tandem:** 1. Security analyst receives the UCM 31.5 report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst opens the report and identifies any exceptions (see '**Anomalies to be followed up on**' below) that need to be followed up on and creates a **Remedy ticket** and assigns it to the appropriate user support group for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **iSeries:** 4. Security analyst receives the UCM 31.5 iSeries alert to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 5. Security analyst assesses the alert and identifies if there is an exception (see '**Anomalies to be followed up on**' below) that needs to be followed up on and creates a **Remedy ticket** and assigns it to the appropriate user support group for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 6. A **logbook entry** is created for tracking of any identified exceptions. If the exception

	based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on (applications/databases):** Follow up activity should be performed on any user id/accounts that appear to be suspicious or where In_ITIM=0 or In_AD=0 with the user's manager or account owner. A whitelist of activity should be developed and maintained by the log reviewers to assist in detecting future anomalies. **Anomalies to be followed up on (iSeries):** Follow up activity should be performed on any privileged, generic iSeries ID such as QSECOFR, QSRV (high risk IBM supplied IDs) to ensure activity is authorized. A whitelist of activity should be developed and maintained by the log reviewers to assist in detecting future anomalies.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 07/18/2017 by Anthony DeMedeiros - Applications Approved on 07/20/2017 by Anthony DeMedeiros - iSeries Approved on 07/24/2017 by Anthony DeMedeiros - Databases
Next Review Date:	July 31, 2018
Review Date Status:	Approved on XX/XX/XXXX by XXX

UCM 31.5a	
Use Case Title:	Successful login to 'Guest' and 'Administrator' accounts
Use Case Description:	Exception based alerts on the successful logins of the 'guest' and 'administrator' accounts for Windows platforms.
Context/Value:	Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Alerts
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives UCM 31.5a alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception (see '**Anomalies to be followed up on**' below) that needs to be followed up on and creates a **Remedy ticket** and assigns it to the appropriate user support group for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on:** For any 4624 event alerts (An account was successfully logged on) that were 'successful' for 'Administrator' and / or 'guest', they should be followed up on and Remedy tickets created immediately and assigned to the appropriate support group for further investigation as this is a non-compliance issue because the 'administrator' and 'guest' accounts should be renamed. For any alerts where the source host is a 'Qualys' scanner, the log reviewers should trend the data on a monthly basis and aggregate the target systems that have been appearing consistently and create a Remedy ticket for further action by the COE support teams (interim approach until the VM infrastructure teams have established a plan for remediation of hardening vulnerabilities).
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).

Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 04/03/2017 by Christine Dewhurst
Next Review Date:	April 30, 2019
Review Date Status:	Approved on 04/25/2018 by Anthony DeMedeiros

UCM 31.5b	
Use Case Title:	Successful login to 'Root' and 'Guest' accounts
Use Case Description:	Exception based alerts on the successful logins of the 'root' and 'guest' accounts for Unix/Linux platforms.
Context/Value:	Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Alerts
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	1. Security analyst receives UCM 31.5b alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception (see '**Anomalies to be followed up on**' below) that needs to be followed up on and creates a **Remedy ticket** and assigns it to the appropriate user support group for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Anomalies to be followed up on:** **Tactical solution:** For any alerts that demonstrate a SSH login or console login (i.e. 'root' was successfully logged on) via 'root' and / or 'guest', they should be brought to the attention of the support teams via email. No direct SSH logins are permitted using 'root' and while console logins are permitted, an authorized Remedy tickets needs to be raised for its use. The tactical solution will occur until the EPS compliance officer follows up with the Vulnerability Management team to determine if they will follow up on direct root logins and guest logins. **Strategic solution:** For any alerts that demonstrate a SSH login or console login (i.e. 'root' was successfully logged on) via 'root' and / or 'guest', they should be followed up on and Remedy tickets created immediately and assigned to the appropriate support group for further investigation as this is a non-compliance issue because the 'root' and 'guest' accounts should be restricted (no direct SSH logins, consoles logins permitted, however, need a valid CR).
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such

	use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	Evidence of tracking, following up and resolution must be retained for at least 24 months (as per IMRR RRS – 1ADM25).
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 04/24/2017 by Christine Dewhurst
Next Review Date:	April 30, 2019
Review Date Status:	Approved on 04/25/2018 by Anthony DeMedeiros

UCM 34.1	
Use Case Title:	Failed logins over time – 'Low and Slow attacks'
Use Case Description:	Exception based reports on Windows, Unix (Solaris, HPUX and AIX), Linux, Mainframe, Applications, Databases, VBOS, Middleware, and Tandem where the failed login is less than 5 attempts over 7 days consecutively which would indicate a potential 'low and slow attack'. Exception based alerts on PostgreSQL, iSeries, and Sybase where the failed login is less than 5 attempts over 7 days consecutively which would indicate a potential 'low and slow attack'.
Context/Value:	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts over time may be an indication of an unauthorized user's attempts to gain access to a system over time by staying 'under the radar'.
Owner:	Director and Head of Technology Business Controls Group
Use Case Review Frequency:	At least annually
Required output:	Exception Report (Unix, Solaris, HPUX and AIX), Linux, Mainframe, Applications, Databases, Tandem, VBOS) Exception Alert (PostgreSQL, iSeries, Sybase, Network Devices)
Recipient(s):	Security analysts (formerly log reviewers)
Actions performed:	**Security Analyst (interim) – Exception Reporting:** 1. Security analyst receives a UCM 34 exception report to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst opens the alert and creates a **Remedy ticket** and assigns it to the user's manager/ID owner for follow up and investigation. Remedy defined SLAs are applied based on the existing Remedy Incident Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up. 3. A **logbook entry** is created for tracking of any identified exceptions. If the exception based report is empty, an entry is made in the logbook and Remedy ticket closed as being 'reviewed'. **Security Analyst – Exception Alert (PostgreSQL, iSeries, Sybase, Network Devices):** 1. Security analyst receives the UCM 34 PostgreSQL, Sybase, Network and iSeries alerts to the LaaS Exception Reporting mailbox: LaaSException.Reporting@bmo.com. 2. Security analyst assesses the alert and identifies if there is an exception. For any identified exceptions, Security Analysts use their discretion to follow up on those IDs that are suspicious and have a high 'event count' based on their historical trending (there are known IDs across various COEs that create noise and don't pose any security related threat but may indicate more of an operational issue. While this use case attempts to filter most of these out, there are instances where the Security Analyst use their professional judgment). Since AD accounts have AD policies applied (i.e. account lockout threshold of 5), the focus of the further investigation will be on the non-AD accounts that have multiple failed login attempts. Some of the IDs with a high 'event count' may be an operational issue that further needs to be followed up with the operational support teams and not considered 'security related'. Any **security** related follow ups/investigations need to be documented in the **logbook** and a **Remedy ticket** created for follow up with the user's manager or other supporting group(s) as necessary (similar to the existing CLM log review process). Remedy defined SLAs are applied based on the existing Remedy Incident

	Management process for **priority** and **target resolution times**. The priority must be **medium** which equates to a target resolution time of **2 business days**. The Security Analyst is responsible for monitoring of the investigation and closure of the Remedy tickets created. For any operational issues, the resolution time may extend past the 2 business days. If the exception requires immediate attention due to a confirmed security incident, the Security Analyst should escalate directly to CSOC IPC ipc@bmo.com and all details of the exception provided to them for further follow up.
Use Case Sanity Validation: *(validating that use case is working as expected in the production environment)*	On at least a semi-annual basis or as required, the use case owner is responsible for testing the use case output in production to ensure the use case is working as expected. Priority of testing should be specific to use cases that are known to consistently produce empty reports or no alerts, to verify that given the appropriate conditions that data would be produced, verifying the integrity and intent of the use case. Testing for such use cases should be performed with the appropriate stakeholders who can perform an appropriate test, in conjunction with established change management processes. Use cases that are known to consistently produce reports and alerts should undergo an examination of a sampling of reports/alerts to provide validation. Evidence of validation should be maintained.
Retention of triage/follow up/resolution:	The original exception reports/alerts along with the evidence of the exception review (i.e. filters applied to extract, logbooks, etc.) are required to be retained for at least 24 months (as per IMRR RRS – 1ADM25) at a minimum. Evidence of tracking, following up and resolution of any exceptions must be retained for at least 24 months (as per IMRR RRS – 1ADM25). Triaging, following up and resolution timeframes are based on the Remedy incident management process and the priority assigned to ticket.
Compliance Monitoring:	The Compliance team is responsible for monitoring the actions of the log reviewers/security analysts and that the log reviewers/security analysts follow the procedures in this LaaS Exception Handling Review Process.
Use Case Status:	Approved on 03/13/2017 by Christine Dewhurst Approved on 06/29/2017 by Anthony DeMedeiros Approved on 07/12/2017 by Anthony DeMedeiros – Mainframe applications Approved on 07/17/2017 by Anthony DeMedeiros – Mainframe zOS Approved on 07/12/2017 by Anthony DeMedeiros – Bluecoat Approved on 07/18/2017 by Anthony DeMedeiros – Network devices Approved on 07/19/2017 by Anthony DeMedeiros - databases Approved on 07/20/2017 by Anthony DeMedeiros – Sybase Approved on 07/24/2017 by Anthony DeMedeiros – IDS (Siteprotector) Approved on 07/28/2017 by Anthony DeMedeiros – Mainframe databases Approved on 07/31/2017 by Anthony DeMedeiros – PostgreSQL Approved on 08/15/2017 by Anthony DeMedeiros – VMWare ESXi Approved on 01/29/2018 by Anthony DeMedeiros – Tandem
Next Review Date:	March 31, 2019
Review Date Status:	Approved on 03/29/2018 by Anthony DeMedeiros